CONDUCTING A FORENSIC INVESTIGATION OF AMAZON DRIVE ON ANDROID DEVICES

A Thesis

presented to

the Faculty of Natural and Applied Sciences

at Notre Dame University-Louaize

In Partial Fulfillment

of the Requirements for the Degree

Master of Science in Computer Science

by

VIRONA NOUHRA

DECEMBER 2018

Notre Dame University - Louaize

Faculty of Natural and Applied Sciences

Department of Computer Science

We hereby approve the thesis of

Virona Nouhra

Candidate for the degree of Master of Science in Computer Science

Pierre Akiki

Dr. Pierre A. Akiki — Supervisor, Chair

H Maalouf

Dr. Hoda Maalouf — Committee Member

Marie Khair

Dr.Marie Khair — Committee Member

Declaration

I declare that this thesis has been composed solely by myself and it has not been submitted in whole or in part, in any previous application for a degree. Except where it states otherwise by reference or acknowledgment, the work presented is entirely my own.

Acknowledgments

First of all, I would like to thank my thesis advisor Dr. Pierre Akiki for his continuous help, support and guidance throughout the work. I also appreciate his efforts in steering me into the right direction to accomplish this work successfully.

I also express my deepest gratitude to my family for providing me with continuous encouragement and support throughout my years of study and throughout this research.

Thank you.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

ADB: Android Debug Bridge

API: Application Programming Interface

dd: data dump Linux command

EDRM: Electronic Discovery Reference Model

IaaS: Infrastructure as a Service

IP: Internet Protocol

nc: netcat Linux command

NIST: National Institute of Science and Technology

OS: Operating System

PaaS: Platform as a Service

PC: Personal Computer

RAM: Random Access Memory

SaaS: Software as a Service

SD card: Secrure Digital card

SDK: Software Development Kit

SQLite: Structured Query Language Lite

su: substitute user identity Linux command

UPM: Universal Password Manager

URL: Uniform Resource Locator

USB: Universal Serial Bus

XML: Extensible Markup Language

Abstract

In the last few years, Cloud Storage has taken a new turn in becoming the latest trend to create a huge impact in the IT world. Amazon Drive is a cloud storage mobile applications created by Amazon. This application provides online and easy access to documents, music, photos and videos saved in your cloud drive. Due to the importance and widespread of the cloud, not only regular users, but also criminals have taken advantage of the services provided by this new technology to commit digital crimes.

Digital forensics is a branch of forensic sciences that aims at investigating digital evidence found on electronic devices to help combat cybercrimes. It aims at identifying, preserving, collecting, analyzing and reporting digital remnants. Digital forensics plays a key role in helping forensic investigators identify valuable and court admissible information.

In this thesis, an analysis is performed on the digital artifacts that are left behind on an Android device after Amazon Drive have been accessed. Methods and tools were used to examine digital evidence, its importance and relevance, to allow examiners to secure the evidence properly.

This thesis follows a four step digital forensic framework to follow a proper forensic investigation process. The results of this process has identified the location of the evidence related to the Amazon Drive account. In addition, the files and folders were identified and in some cases the content of some files was retrieved. This thesis showed that deleted files can also be acquired.

Keywords: Digital forensics, Cloud Computing, Cloud forensics, Mobile forensics, Amazon Drive analysis.

Chapter 1: Introduction and Problem Definition

This chapter provides an overview of the field of cloud computing, Amazon's cloud mobile applications, and the field of digital forensics. The general problem is also defined and explained in order to highlight the significance of this work in the field of cloud forensics and in helping forensic investigators. The research objectives, methods, and procedures are stated and explained. An overview of the main results is also provided.

1.1 Introduction to the General Problem

The way we perceive the world has been totally modified by the vast intrusion of technology around us. The internet and information technology have become essential elements in our daily life, whether at school, work, home or any other place. It is undeniable that this invasion brought a great deal of services to help facilitate people's lives. One of these services is cloud computing.

Cloud computing is one of the latest trends in technology as defined by the National Institute of Science and Technology. It's widely accepted definition states that "*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models*." (Mell & Grance, 2011)

In other words, cloud computing offers users the ability to benefit from available resources anywhere using any device capable of accessing a cloud platform in the easiest way possible. Using cloud computing, a user does not only benefit from storage services but also from the availability of tasks such as sharing files, pictures, documents, getting access to different programs and software on devices with limited RAM and processing power, in addition to the ability to synchronize calendars and contacts. These services provided by the cloud are categorized into three service models. The first service model is Infrastructure as a Service (IaaS) that provides virtual hardware such as servers, networks and storage that helps users build a virtual infrastructure with the same functionality as a physical one. Two notable examples of IaaS are Amazon Web Services[1] and Microsoft Azure[2]. The second service model is Platform as a Service (PaaS) where methods for tools to be developed are provided to easily interact with databases, web servers, and file storage. The user manages building the application and does not deal with the complexity of the infrastructure, software licenses and development tools. Google App engine[3] and Salesforce[4] are examples of PaaS. The third service model is Software as a Service (SaaS) where the cloud service provider offers a complete software solution using the "pay as you go" purchase model. Office Web Apps[5] and Google Drive[6] are examples of SaaS.

Due to all the services that cloud computing offers, its popularity has greatly increased. With the evolution of smartphones, accessing cloud storage services has spread even more. In 2016, the world's largest research firm, Markets and Markets, estimated that the cloud storage market will grow to USD 74.94 Billion by 2021 (Markets&Markets, 2018). Cloud computing is not only for businesses and large organizations, but it has become in recent years available to all types of consumers due to the development of mobile cloud applications. Amazon Drive is a widely used cloud mobile application that offers online storage utilities. The forensic investigation conducted in this thesis will use this application.

Amazon Drive provides easy access to the documents, music, photos and videos that you have stored on the cloud. It also allows its users to view, share and save content, even if

[1] https://aws.amazon.com/

[2] https://azure.microsoft.com/en-us/

[3] https://cloud.google.com/appengine/

[4] https://www.salesforce.com/

[5] https://www.office.com/?ms.officeurl=webapps

[6] https://www.google.com/drive/

their devices get lost or damaged. Amazon Drive permits its users to perform a series of tasks such as previewing the content of documents, playing music and videos, creating and editing texts, sharing files, and so on (Amazon, 2016b). It also offers free unlimited photo storage for Prime members, other storage plans start at 11.99$/year (Amazon, 2016c). Amazon Drive, does not only support cloud storage capabilities, but it also supports many features that give cloud applications an undeniable value in the technological world. These features include: files storage that can be accessed anywhere, safety, security and, content back up. Amazon Drive also allows its users to free up space on their devices and allows them to easily search for content through a usable interface. (Amazon, 2016a)

The introduction of cloud computing applications combined with the increasing usage of smartphones worldwide, created a huge flux of information on mobile phones. This phenomenon transformed mobile devices into a target for cybercriminals to use for illegal purposes. Cloud applications are becoming more at risk of attacks and being used to hide information related to actual crimes, hence, pushing forensic examiners to look beyond physical storage devices and starting with examining applications with a storage on the cloud. The whole procedure of examining devices in case of an illegal crime is a very delicate process in order to locate and correctly preserve the evidence needed.

1.2 Problem Definition

With the increasing usage of mobile cloud applications, cybercriminals and terrorists are more likely to take advantage of any new technology to commit crimes.(Marturana, Me, & Tacconi, 2012). The access to cloud computing applications on smartphones has increased its popularity and at the same time raised questions concerning security and privacy issues. A report by Symantec stated that the number of Android apps classified as containing malware increased by 230% between 2014 and 2015. This report also stated that the volume of Android variants increased by 40% in 2015, compared with 29% growth in the previous year (Symantec, 2016). This is a clear indication that smartphones are not as safe as they should be, and that malwares are putting personal information stored in the cloud at risk of being stolen by malicious hackers. An example of this case is the leaking of multiple celebrity personal photos stored in iCloud in 2014 (Duke, 2014). In addition, cloud storage applications could be used by criminals to store incriminating records. For instance, a user saving pictures related to child pornography or records about drug deals could provide enough evidence to be used in court. These issues affect the way digital forensic examiners tend to assess an online crime. For example, in 2011 and according to Kaspersky security firm, cybercriminals were spreading the malicious Trojan horse, Spy Eye, by hiding it in the Amazon storage service (Scott, 2011). For many years, people were using traditional storage devices, such as hard drives and optical discs, but with the introduction of the cloud users are less likely to store local copies of documents on the hard drives of their computers and electronic devices, given all the benefits provided by the cloud (Marturana et al., 2012). Although, it is possible to retrieve the stored information from the cloud service provider, this has created a new challenge for forensic investigators because the process takes a lot of time. In addition, knowing that cloud architectures store data in many different physical locations around the world, the procedure can be blocked by overseas jurisdictions(Grispos, Glisson, & Storer, 2013).

These challenges can slow down the process of retrieving, preserving and analyzing digital evidence in a timely fashion. Hence, more research is needed in the field of digital forensics to support investigations in finding more evidence and reaching more accurate conclusions.

1.3 Research Objectives

The aim of this research is to help forensic investigators in finding digital evidence using a proper forensic approach and to answer the following research question:

What are the digital artefacts that remain on an Android phone running Android 6.0.1 Marshmallow operating system after the user has used the Amazon Drive cloud application?

In order to answer the research question, this thesis focuses on determining an admissible method capable of collecting valuable digital evidence from a smartphone running Android 6.0.1 Marshmallow OS, in a forensically sound manner while maintaining the integrity of the evidence. The research aims at exploring the traces that are left behind after a user has accessed and used the Amazon Drive cloud account.

This thesis aims to provide forensic investigators with the type, significance, and location of digital evidence on an Android phone. It will make the work of investigators easier and faster, since no similar research was previously conducted on Amazon Drive. This thesis will inform investigators on how to look, examine, and search for digital evidence efficiently.

1.4 Approach and Main Results

For a forensic investigator to conduct experiments and identify potential evidence on the smartphone, it is necessary to have an understanding of the internal structure of the device. Therefore, the original work conducted started by reviewing the file hierarchy in the smartphone to locate the partitions in which the evidence might be stored. Then, a set of experiments were setup. Those experiments represent the set of actions performed by a user while using the application. A digital forensic framework was used to conduct the investigation.

The forensic framework is composed of four stages. The first step consists of identifying the source of evidence and preserving it. The following step comprises the collection of an image which contains the evidence from the device. Afterwards, the collected image is examined and analyzed using an appropriate tool. At last the results are written in a report.

The findings of this thesis show that a forensic investigator is capable of retrieving deleted files, extracting the content of documents as well as images. It also helps in identifying what type of artefacts can be collected in each activity. Additionally, the results state the location of the evidence and give examiners timestamps that are very valuable to an investigation.

1.5 Thesis Organization

The structure of the work in thesis was divided in to several sections. The first section described the general problem and the challenges faced by the field of digital forensics. The first section also comprised the objectives of the research conducted and the research question that needs to be answered. A general overview of the thesis and the main results were also presented.

In the second section, a definition of the basic concepts in digital forensics were highlighted for a better understanding of the technical concepts. This section provided an explanation about mobile forensic, the importance of evidence and extraction techniques. The digital forensic framework used as well as the tools used throughout the investigation are well defined. In addition, this section holds within it the literature review which covers the challenges of cloud forensics, the frameworks in digital forensics, the research done in cloud forensics on personal computers and smartphones.

The third section is related to original work. It comprises an explanation of the Android smartphone file hierarchy and the set of experiments conducted which reflect a user's activity on the device. In addition, a detailed explanation of the actions performed in each step of the framework with the results are described in details.

The last section of the thesis is a conclusion. It briefly summarizes the work done and the acquired results. Additionally, the contributions are presented combined with possible extensions to the work in the future.

Chapter 2: Background and Motivation

In this chapter, basic concepts related to digital forensics are clearly defined to provide a better understanding of the technical terms and their context. Then, the tools and set of techniques used to conduct investigations in the field of cloud forensics are described and explained. In addition, a detailed literature review is conducted on the previous research done in the fields of cloud forensics as well as mobile forensics. Finally, the motivation and objectives of this work are presented.

2.1 Definition of Basic Concepts

With the increasing usage of smartphones and tablets worldwide, online threats are no longer limited to computers, cybercriminals are expanding their attacks to reach smartphone devices which are the equivalent of a computer. According to Nokia's threat intelligence report, smartphone infections increased by 400% between January and December in 2016 (Nokia, 2016). Cybercriminals know that our smartphones upload to the cloud a huge amount and a variety of valuable personal information that includes: bank account numbers, emails, documents, pictures, and so on. Attackers take advantage of all the possible ways to access smartphone devices and find critical information that allows them to control a user's personal information. Mobile applications leave behind digital traces just like a murderer leaves behind physical evidence in a crime scene. The evidence found on the smartphone of a suspect or a victim is vital in finding not just cybercriminals but also criminals that have used a smartphone to contact the victim and commit the crime.

Almost every single person owns a smartphone loaded with social media applications on which she or he documents their daily activities. Cloud applications, that help them back up their most valuable documents and personal pictures, are also becoming integral part of their daily activities. In addition to other kinds of applications that give an insight about their preferences and activities. Hence, smartphones are devices loaded with valuable data.

This indicates the importance of the field of digital forensics in collecting and understanding all the digital evidence produced by these applications to better understand the user's activities, preferences, lifestyle and mindset in order to solve either a crime or a cybercrime.

2.1.1 The field of digital forensics

The field of forensics was the central part in investigating crimes ages ago. When cybercrimes emerged, digital devices became an integral part in solving cases thereby leading to the introduction of the field of digital forensics. Let us start by defining digital forensics which is the science equivalent to classical forensics, where evidence analysis takes place using data extracted from any kind of digital electronic device (Barmpatsalou et al., 2013) . In simpler terms, digital forensics aims at collecting, analyzing and preserving digital evidence retrieved from digital devices such as: tablets, computers, smartphones, and so on. This evidence is collected and analyzed in a sound manner using tools and frameworks, and then it is presented to a court of law. An entire profile of the victim as well as the criminal can be built for a clearer vision of the character as well as the motives behind the crime. A small example is the 2007 shooting of dozens of people on the campus of Virginia Polytechnic Institute when the forensic investigators got hold of the shooter's computer and built a psychological profile that helped understand the shooter's state of mind. It was after this incident that the police understood the importance of analyzing digital devices (Noyes, 2014).

Since digital evidence can be found in different places in a digital device as well on the network it is connected to, many sub disciplines were created such as: computer forensics, memory forensics, network forensics, mobile forensics, and so on (Eoghan et al., 2011). Mobile forensics is the sub-discipline that is the most relevant to this thesis.

2.1.2 Mobile forensics

Technology revolutionized mobile phones and created powerful smartphones capable of performing tasks as well as storing personal and sensitive information. This revolution affected the field of digital forensics. It has encouraged forensic investigators, not to get hold of personal computers only for analysis, but also any smartphone found in the crime scene. As smartphones can highly contribute to the proceedings of the investigation.

Mobile forensics, one of the divisions of digital forensics, is the science of recovering digital evidence from a mobile device under forensically sound conditions using accepted methods (Jansen & Ayers, 2007). This implies following the process of collecting, preserving, analyzing, examining, and presenting the data found on a device to the court of law without damaging or changing the evidence.

Knowing that each smartphone belongs to a single individual helps in revealing a lot of personal information and identifying key evidence in a crime. For instance, with the use of a spy software, the mobile device can compromise the life of their owners by working against them. A smartphone containing a spying tool, without the owner's consent or knowledge, can be used to eavesdrop on phone calls, text messages, emails, pictures, videos, and social media applications.

Many cases involve the illegal interception of communications through the use of spyware. For example, one person knew a lot of intimate details about their business partner that the victim swore only shared with his attorney. Both the attorney and his client suspected an interception of communications was happening, so the victim's computer and cell phone were sent for a digital forensic examination and the results showed evidence of a spyware installed on the smartphone (Melson, 2014).

These cases show the importance of digital forensics and, mostly, digital evidence in solving a digital crime. Digital evidence gives insights about the cloud account users by providing information about photos, documents, videos and their timestamps. It is clear that mobile forensics is a valuable source of digital evidence for forensic investigators.

2.1.3 Digital evidence

Digital evidence can be used in any serious criminal investigation such as: rape, abuse, murder, piracy, property theft, and so on. It can offer a very useful insight into the victim as well as the criminal's activities before and after the crime. For instance, a criminal could be using Google Maps before committing the crime could tell forensic investigators about his whereabouts, or text messages could identify possible suspects who may have threatened the victim, or a thief could be posting pictures of stolen items on websites such as eBay. In any of those cases, there is always an electronic trail left behind for forensic investigators to collect, preserve and examine using appropriate tools and methods; not following a set of procedures can yield to loss or damage of evidence that will no longer be admissible in court (Carter, 2014).

Digital evidence is both sensitive and fragile, it comes in many types on electronic devices. There is the kind of evidence found on the internet such as the information retrieved when searching through communication websites like chat rooms. Another source of information is the file sharing networks that allow users to share illegal material. The second kind of evidence is the one found on computers' hard drives and memory such as a log file containing the user's activities in addition to files and folders (documents, videos, songs, presentations…) that a user stores on his/her hard drive which are of great forensic value. The third and most important type of evidence for this thesis is the evidence found on portable devices particularly mobile phones. The growing power and storage capacity of smartphones would give more useful data such as metadata, detailed information about a piece of data like a document or a picture, which provides an additional layer of information about the file such as the location, time and date(Goodison et al., 2015).

2.1.4 Techniques and tools for data extraction

Knowing the value of digital evidence and its fragility, it must be handled carefully using a set of predefined techniques and tools to extract the data and analyze it. Before doing so, forensic investigator must keep in mind the forensic soundness of the collected data, meaning that the forensic investigator ought to minimize the modifications made to the device. Then, he must ensure the integrity of the evidence is intact by placing the smartphone found on the crime scene in a Faraday bag that creates a radio suppressed environment to avoid the device being remotely wiped over a mobile or WI-FI network.

The diagram presented in Figure 2.1, shows how digital evidence may be extracted from a smartphone device. Each stage requires a different set of equipment, expertise and technique to obtain the data. Extraction techniques vary from manual which are the simplest methods. They consist of using standard inputs available in the device like a keyboard or a touch screen. It does not require any special skills, only knowledge of operating systems and file structure. The limitation of this techniques is that it cannot retrieve deleted file clusters through the use of a standard interface.

The second technique is logical extraction of evidence. It requires the use of commands through code to target the device. A forensic investigator can use tools that connect to the device and displays extracted data on the examiner's computer. This technique requires more knowledge and skills.

Physical extraction techniques read data directly from memory. Memory is the location where a device saves a list of actions either read or write information. On this level, physical extraction, deleted files can be retrieved. This level is more difficult to handle and requires greater experience and more sophisticated tools and techniques.

The last two techniques are micro read and chip-off, both are very technical techniques that represent an advanced level of digital extraction. Reading information is directly done through the memory chip. Handling those techniques can be slightly difficult and requires a lot of expertise in the field (Goodison et al., 2015).

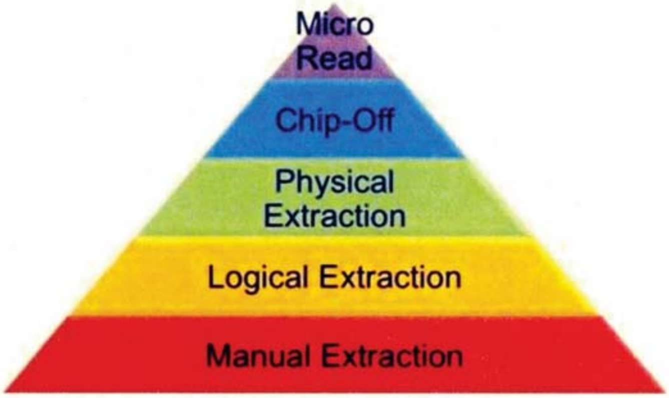


Figure 2.1 NIST Mobile Extraction Classification (Ayers, Brothers, & Jansen, 2014)

In order to extract evidence in a professional and sound manner without damaging it and compromising it, there is a need to follow a set of predefined guidelines, frameworks and tools. Those are discussed in detail in the following section.

2.2 Frameworks and Tools for Extracting Digital Evidence

Section 2.1 introduced the field of digital forensics, as well as mobile forensics and showed the importance of this field in solving crimes and cybercrimes. Section 2.1 also discussed the importance of digital evidence and the different ways for extracting it from electronic devices.

To conduct a sound and accurate digital investigation, there is a strong need to follow a set of predefined guidelines and frameworks to make sure that the collected digital evidence is admissible in a court of law and abides to the digital forensic principles of data correctness, preservation and integrity.

The most important set of guidelines are the guidelines on mobile device forensics defined by the National Institute of Standards and Technology which are integrated in the conceptual evidence collection and analysis methodology for android devices published in 2015. This methodology provides an in depth guiding manual for forensic investigators to conduct their work. The methodology is composed of the phases presented by the following subsections.

2.2.1 Evidence source identification and preservation

This phase is mainly concerned with identifying sources of evidence in an investigation and preserving it for examination and analysis. During the process, an investigator identifies electronic devices of forensic value such as smartphones. The device should be placed in a Faraday bag to prevent the device from being remotely accessed which could compromise the evidence and manipulate the outcome of the investigation. If it is not feasible to place the device in a Faraday bag, it should be placed in airplane mode to disable the device's radios.

Any cables attached to the device such as a charging cable should be placed with the device. The needed photographs should be taken of the device and its attachments in the crime scene.

The practitioner on the scene should be able to determine the approximate Android version of the device through visual artifacts on the lock screen, if the device is locked. It is important to identify the device by looking for the model, manufacturer and other labels and specifications usually available on the back of the device.

The process should also include a logical collection of volatile memory of the Android device, even though this extraction technique does not provide as much data as the physical collection, it retrieves valuable information that can be lost once the device is powered off such as encryption key, in case the device was encrypted.

After performing the list of procedures, the device can be powered off and the next phase can start.

2.2.2 Collection

In the collection phase, knowing that the volatile data in memory was collected and evidence was preserved, the forensic investigator's job is to collect a physical image of the device's "userdata" partition, which contains the nonvolatile data. The physical collection strategy allows the forensic investigator to collect all of the files on the partition where most of the evidence is stored. It also helps in recovering files that were deleted by the user from unallocated space and in performing keyword search using forensic tools.

Cloud applications are different from other types of application, with respect to sorting their data in data centers that could be outside the jurisdiction of a country. Even if the data centers were within a country's jurisdiction, the forensic examiner would be required to provide a warrant and contact the provider of the cloud service to request information about a user's account. This procedure takes a lot of time and may not yield any results since the cloud service provider can deny access to a user's personal information.

Therefore, the goal of forensic investigators is to collect the digital evidence left behind on a user's smartphone as fast as possible (Martini & Choo, 2012).

After identifying the source of digital evidence, preserving the device in a safe environment and collecting the logical and physical image of the device's partitions, it is important to maintain the integrity of the collected evidence and thus perform a hashing over the collected image. It is recommended that the practitioner uses a hashing tool on the device's flash block file and on the collected image available on the PC. The result should be identical hash values. In case the values are not identical then the data has been tempered with. This part of the process is integral for documentation and for the reporting in a court of law.

2.2.3 Examination and analysis

After performing all the necessary tasks to collect evidence from the partitions of the device. The forensic investigator will move to the examination and analysis phase of the process. This section is dedicated to analyzing the images that were extracted from the device and take a closer look by identifying valuable digital evidence. The forensic examiner will detect remnants of user activities after the use of the cloud application.

The first step is to determine the installed application that is of interest for this investigation. This stage allows the practitioner to use tools to conduct a search for keywords on the physical image and retrieve more detailed results for a particular application.

Throughout this phase, the practitioner examines the application's private storage, also known as the application's data directory. Most of the evidence is found in this directory while examining the files. Another location to examine is the external storage of the android device, located on a physical SD card inserted into the device. Other files that should be examined are the database files of the application. Android supports SQLite but this does not prevent other applications from using different databases. Cloud application use online services that require authentication, and thereby choose to store their credentials in a database provided by the OS AccountManager service. After all of the abovementioned data is examined and analyzed, the practitioner moves to the stage of reporting and presenting.

2.2.4 Reporting and presentation

At this stage a summary of the findings and a presentation of their digital forensic value in the investigation are shown. The practitioner also presents the details of the techniques used to collect, examine and analyze the evidence and they may include data that they derived from analysis.

2.2.5 Tools

As the steps of the framework are explained, we noticed that some of the tasks can be completed using forensic tools. To facilitate the work, achieve faster results and have a better understanding of the role of each tool, the tools used throughout the work are presented below.

- **Android Studio and SDK tools** are a set of tools, developed by Google Company, that provide a development environment to build Android applications. One of the tools is ADB, Android Debug Bridge, a command line tool which allows you to communicate with an Android phone using a PC (Morum de L. Simao, Caus Sicoli, Peotta de Melo, & Timoteo de Sousa Junior, 2011).
- **Autopsy** is an open source mobile forensics tool created by Basis technologies. Its role is to analyze the extracted images from an Android phone.
- **SQLite Database file viewer** allows forensic examiners to study database files that they may find on Android devices which use SQLite Database files.
- **SuperSU** is an application that manages the root permissions for the installed applications on a smartphone.
- **Busybox** is an application that provides examiners with command Linux commands that are not installed on Android by default.
- **Odin 3.10.6** is a tool that allows examiners to root a smartphone.

2.3 Previous Work on Digital, Cloud, and Mobile Forensics

The following section discusses the work previously done in the field of digital, cloud and mobile forensics. The challenges and limitations associated with cloud and mobile forensics are discussed in Section 2.3.1. The frameworks used throughout an investigation process to conduct a sound investigation are discussed in Section 2.3.2. Section 2.3.3 discussed cloud forensics and is divided into subsections that presented the work done on cloud applications on computers and mobile devices. Section 2.4 presents a few research papers related to the collection of digital evidence from cloud applications.

2.3.1 Challenges in cloud forensics

This section provides a brief overview of different research papers that have discussed the challenges encountered in the field of cloud forensics. Researchers aim to address these challenges in order to support better digital investigations.

(Barmpatsalou et al., 2013) provide an overview of mobile forensics by presenting and reviewing the main milestones, methodologies and significant studies throughout the last seven years. A timeline displaying the most important contributions in the field show the evolution of mobile forensics in the case of different mobile operating systems. Their work also presents the challenges and issues faced by investigators such as the need to be aware that different operating systems and different smartphones exhibit different behaviors while collecting digital evidence. Therefore, investigators need to stay up to date to the different updates and changes in devices.

Choo et al. (2016), highlight the growth seen in the research work related to cloud forensics and emphasize that both cloud forensics and mobile forensics are under researched topics, since there aren't enough publications. Additionally, there are issues that investigators need to address. These issues include staying up-to-date with the newest software and hardware modifications on devices and the anti-forensics techniques and tools used by cybercriminals to impede the work of forensic investigators (K.-K. R. Choo et al., 2016).

(Ruan et al., 2011), introduce the field of cloud forensics from legal, organizational and technical dimension and then presents a list of challenges which are almost the same as the ones presented by (Simou et al., 2014). The latter one divides the challenges according to the different stages of the frameworks (data acquisition, preservation and collections stage, analysis and presentation stage) similarly to (Shah et al., 2014). One of the listed challenges are the lack of qualified personnel to handle and analyze digital evidence. Another challenge is the problem of multi jurisdiction since the data stored on the cloud could be stored on servers in different geographical locations. In other words, physically accessing those servers and retrieving the data can compromise the privacy of other users and requires a warrant from the country that hosts the server to give access to forensic investigators. All these procedures delay the process of collecting evidence giving more time for cybercriminals to delete data and hide their traces.

Other research papers highlighted the different challenges of cloud and mobile forensics and proposed solutions. (Samet et al., 2014) listed the challenges in addition to references to solutions provided by other researchers. (Damshenas et al., 2012) presented challenges were associated with solutions according to each stage of the framework but with (Birk et al., 2012) each issue presented was linked to a proposed solution.

This overview of the challenges in mobile cloud forensics demonstrates the aspects of the field that need improvements and more research which has encouraged this work.

2.3.2 Frameworks for digital forensics

To avoid digital evidence being called into question in judicial proceedings there should be a set of guidelines and procedures to conduct forensic investigations, examinations and analysis of digital evidence. Those guidelines and procedures are known as digital forensics frameworks. In this section, an overview of the frameworks used in cloud and mobile forensics proposed by researchers are explained.

(Martini et al., 2012) proposed an integrated conceptual digital forensic framework in cloud computing based on the widely adopted frameworks of McKemmish (McKemmish, 1999) and NIST (Kent et al., 2006). The newly proposed framework adapted the previous ones to the changes in digital forensics and offer better guidance for investigators. The framework is divided into four stages. The first stage is evidence source identification and preservation, which is concerned with locating valuable evidence and preserving it properly to prevent it from being damaged. The second stage is concerned with collecting the data needed using the appropriate techniques. The third stage is examination and analysis that focuses on understanding the meaning of the collected data and trying to find additional evidence, leading to an iteration of the process since, the investigator might be able to identify new sources of evidence and collect new data. The fourth stage is reporting and presenting the digital evidence in a clear format. Being able to perform iterations in this framework is what it makes different from previously proposed ones.

The previous framework is used as an underlying guiding environment for the work done by (Martini et al., 2015) and thus the four stages of the process (evidence identification, preservation, collection, analysis, examination, reporting and presenting) rely on in their work. The aim of this research is to present a methodology that is practical, device agonistic, and adheres to the laws of forensic soundness of evidence. The major contribution of the work is a very detailed process of eight steps explaining how to collect evidence in a forensically sound manner. Martini and Choo's methodology includes techniques to bypass the security of the device and OS as well as create a bit for bit image of the partitions in the device and analyze the retrieved evidence.

In another research done by (Quang et al., 2015), researchers proposed an adversary model that can be easily adapted to the latest mobile device technologies to facilitate forensic investigations. The model takes into consideration the principles of forensic soundness and applies them on the adversary. The paper presents the adversary model and a construction of the model, Android evidence collection and analysis methodology, which ensures that practitioners conduct investigations in a forensically sound manner. In the model, there exists an adversary with physical access to a mobile device and the ability to exploit the vulnerabilities in the device's security system. The adversary, in this case the forensic practitioner, aims at collecting confidential data from the device while respecting the principles of forensic soundness. Some of the different options that allow the practitioner to exploit vulnerabilities are exploit and modify, inject, forensic copy, transmit and many more. Researchers have discussed how these set of instructions fit in the constructed evidence collection and analysis methodology for mobile devices.

In the research done by (Do et al., 2015), researchers have found, after an overview of the literature review, the need to build a forensically sound methodology to collect cloud based evidence from Android devices. The cloud focused mobile forensics methodology is based on the previous work done by the same researchers, in conceptual evidence collection and analysis methodology.

The methodology highlights the four basic stages of the framework, evidence identification and preservation followed by evidence collection where researchers setup bootloader for live OS, boot live OS into memory and collect physical images of the partitions of the device. In the third stage of evidence identification and analysis, files in the external and internal storage of the device are examined as well as the database files and the accounts examined and analyzed. The last stages handles reporting and presenting the results.

The methodology was applied on three cloud applications, Box, OneDrive and Dropbox, which were installed on an Android smartphone. The results described the findings of the investigation.

2.3.3 Cloud forensics

In the following section of the literature review, the contributions and the shortcomings of the research previously done in the field are elaborated. For a better understanding of the diversity of the research in digital forensic, this section was divided into four subcategories: research in cloud forensic performed on computers, research performed on both computer and smartphones, research done on smartphones only, and finally additional research done on the cloud.

2.3.3.1 Cloud forensics on computers

This section presents an overview of the state-of-the-art in cloud forensics on cloud applications installed on computers.

In 2012, a research aimed at adapting methods and techniques in traditional digital forensics to performing investigations in cloud environments. The researchers built a case study based on a set of SaaS applications, document editing and photo sharing applications such as Google Documents, Picasa Web and Flickr with the aim of demonstrating that enough evidentiary data can be retrieved to prosecute a criminal in court. Analysis of those applications demonstrates that potential evidence might be found in internet cache, logs, temporary files, navigation history, downloads and cookies of the web browser. For the research five different scenarios were created. The first four cases consisted of performing test scenarios on the applications (Flickr, Google documents, Picasa Web and Dropbox) accessed via three chosen web browsers: Internet Explorer, Google Chrome and Mozilla Firefox. The fifth case was testing the Dropbox application installed on the client's personal computer. Using forensic tools, an inspection of the local folders and web browsers databases showed that in some cases, researchers were capable of retrieving the information about the log in phase, a copy of the downloaded files, the filename, cookies and images. All the collected evidence was recovered from local artifacts found on the device without having to access the servers (Marturana et al., 2012). However, the research was performed only on a limited number of web browsers on a personal computer, and no test scenarios were performed on smartphones. The findings of the test performed on the Dropbox client software were not detailed and the results of the sniffing done over the network was not shown.

Another research, conducted by Kurt Oestreicher, aimed at answering several research questions in order to determine the kind of data of forensic value that can be collected from an iCloud application on a Mac OS. The research tried to locate the iCloud-synched files on the OS, worked on checking the integrity of the data using MD5 checksum and determining if the collected files were the same as the original ones. The research also outlines where the user data is located on the OS. It was concluded that the files found were the same as the original and the acquired timestamps were not modified (Oestreicher, 2014). Even though this research was helpful in determining the location of key evidence and establishing the integrity of the files, it was limited by the version of the OS. Also, the forensic examination was only performed on a computer, while iPhones and iPads were not considered.

(Hale, 2013) discusses the digital artifacts left behind on a computer after a user has used Amazon Cloud Drive. The testing performed was through the desktop application as well as through the web browser on two operating systems: Windows XP and Windows 7. Two Perl scripts were created to facilitate the process and reduce the time needed for an examiner to manually collect digital artifacts from Amazon Cloud Drive. Hale's research showed the kind of artifacts that can be retrieved from an online interface, they are the file name, type, size, date, deleted files and their deletion time. As for Amazon Cloud Drive application, it was possible to carve files from unallocated space using cloud drive artifacts. Even though the research did make remarkable contributions, it was only performed on a computer and using one of the earliest versions of the application.

(Blakele et al., 2015) provide an insight on the data remnants left behind on a Windows 8.1 computer after the hubiC cloud service has been installed and manipulated through different scenarios. In the experiment setup, the web browser based experiments were done using three web browsers: Internet Explorer, Google Chrome and Mozilla Firefox. Experiments were also conducted on hubiC desktop application and a sample of the Enron dataset was used. After the experiments were conducted, a thorough examination and analysis of the findings was performed and the following evidence was found: username and password of the user were retrieved as well as a deleted file, security systems and IP addresses of the hubiC servers were also detected after an analysis of the network traffic which could cause security risks for the user. Knowing that this research presented valuable insights to forensic investigators, it did not include any research performed on smartphones and the work was limited to a specific operating system.

A study conducted in 2017 performed a series of tests on two cloud applications, iDrive and Mega Cloud, to give an idea to forensic investigators about the kind of evidence that remains on a user's computer after the use of these two cloud applications. The aim of the study was to identify and locate evidence on storage media of a computer running the Windows 7 operating system after the user has manipulated the applications either through the installed cloud application or through these web browser: Internet Explorer, Mozilla Firefox and Google Chrome. Researchers also tried to identify evidence from network traffic and check the timestamps of the files on the cloud application. After performing the necessary examination and analysis on memory, browser logs, registry files and hard disks, it was possible for forensic investigators to acquire the user's profile details, machine's username, username and password for iDrive cloud and the cloud provider name and customer's profile details such as username and password for Mega cloud (Thamburasa et al, 2016). The study offered a valuable contribution to the filed. However, the work was limited to a personal computer and to one operating system only.

Due to the lack of knowledge about the location of the evidence on electronic devices which could lead to a slow investigation, (Easwaramoorthy et al., 2016) performed a forensic investigation on two cloud applications, Amazon Cloud Drive and Microsoft One Drive, through a web browser and a client application installed on a Windows 7 computer, to tackle this issue. The goal was to clearly identify evidence of forensic value for practitioners on a client machine. Using the digital forensic process of identifying, preserving, collecting, analyzing, examining and reporting the presence of evidence, investigators acquired evidence from RAM and the hard disk by creating different virtual machines that would imitate the work of three different web browser: Internet Explorer, Google Chrome and Mozilla Firefox. The results showed that information about the service provider and the user account details were recovered, most of the artifacts were found in database files, system configuration, log files and setup files. The username and password of the OneDrive client were identified as we~~ll~~ as the computer name, cloud service provider details and user account details were also identified after the analysis of Amazon cloud drive generated artifacts. As previously noted, this study is only limited to two cloud applications on a Windows 7 operating system and the results are only specific to that case and do not apply to other cloud applications in different settings.

Using two of China's cloud storage services, Baidu cloud storage service and 360, as case studies, Long and Qing discussed the type of artifacts that might be left behind on a user computer running a Windows operating system. Researchers aimed at collecting artifacts from both the client software on the machine and through the web browser, Internet Explorer. Since researchers handled a case study of an employee suspected of copying and stealing files, they applied the methodology of collecting the evidence and ended up with information about the employee's activities and the copied files, they also analyzed timestamps which resulted in valuable clues for the investigation. This research provide a method capable of reconstructing a user's activity, it can associate traces left behind and rebuild the user's actions on the cloud application and provide further clues for the investigation(Long et al., 2015). This research was limited to artefacts that could be found on a computer with Windows operating system even though the suggested method could be used in different case studies.

The research conducted by Quick and Choo explores the process of collecting data, in a timely fashion and preserving it. The data was collected from three popular cloud storage applications (Dropbox, Google Drive and Microsoft Skydrive). This study was conducted through the use of web browsers and client software and then the analysis was performed on the collected evidence. It was determined that there were no changes made to the content of the files during the processes of upload, download and storage performed on the three cloud applications. Regarding the timestamps of the files, which offer a lot of valuable information in the course of an investigation, it was noted that some of the timestamps remained unchanged during the download, upload and storage of files via web browser and via client software(K.-K. R. Choo et al., 2013). Since timestamps and the content of files can be altered by performing certain actions, this study showed the timestamps and the content that remains the same throughout the process. However, the results are not accurate for new releases of the client software because the way files are downloaded, uploaded or stored can change in the future. Additionally, cloud storage providers may change the way time and date is stored for the files, which could alter the timestamp information of the file.

2.3.3.2 Cloud forensics on computers and mobile phones

This section presents research papers concerned with cloud forensics applied on computers and mobile phones.

A research focuses on gathering evidence from devices running Ubuntu and Android OS, and computers running Windows 8.1 to locate digital artifacts left behind after the use and deletion of cloud applications. On Windows 8.1, researchers performed experiments through Google Chrome to identify artifacts left behind once a user accesses a cloud application. They also identified digital evidence that remains after the user installs and manipulates Copy, ownCloud and Dropbox cloud applications. They also performed an analysis to try and retrieve deleted files from unallocated space and an analysis on the physical memory. Additionally, further research was conducted using Mozilla Firefox on Ubuntu and on the main directories of the client applications (Copy, ownCloud and Dropobox) and analysis was performed on physical memory and to retrieve deleted files. Part of the research was dedicated to acquiring digital evidence from Android operating system which are based on Linux. This study offered a great deal of evidence in cache files, log files, database files, inside memory and the registry that can help forensic investigators in locating evidence in faster way (Malik et al., 2015). However, this research was only limited to three cloud applications on Windows, Ubuntu and Linux. This research did not expand to other operating systems of smartphones such as iOS and with a new version of the client software and operating system, and therefore it needs an update.

(Martini et al., 2013) conducted a set of experiments to identify the set of artefacts of forensic value to practitioners on both the client side and the server side. The experiment on the client side was conducted on a Windows operating system using three major web browsers (Internet Explorer, Mozilla Firefox and Google Chrome) and the ownCloud client application. Further work was done on an iPhone with an iOS version 5.1.1. Additional forensic analysis was conducted on network traffic and then on the server side of the cloud storage provider. Artifacts generated on the client side came from file metadata, sync files, database files, and folders and accessed files. The artefacts on the server side were found in the SQL database, data directory, file versioning, and web server logging data. The analysis of these artefacts provided insights to forensic investigators about the username, the files uploaded, deleted and downloaded, server file name, directories of files, logoff events, encryption key and many more valuable information. Even though, this paper presented work on both client and server side, the research was only limited to a specific cloud application and on iOS operating system for smartphones.

In 2013, Quick and Choo conducted a research aiming at identifying digital evidence of Microsoft SkyDrive, a cloud storage application, that are likely to remain on a client's machine and over network traffic. The experiments were conducted on a computer running Windows 7 using a web browser (Internet Explorer, Google Chrome, Mozilla Firefox, and Safari) and a client software, and on an iPhone 3G smartphone where SkyDrive is accessed either through the Safari web browser or through a the SkyDrive iOS application. The Enron dataset was used in these experiments. Researchers tried to determine the artefacts that might be left behind after a client used anti-forensic tool to hide evidence and delete it. The outcome of this research was identifying cloud service and user account details, as well as, username and password, sample files and their timestamps. In the case where anti-forensic tools, Eraser and CCleaner did not remove all the data and part of the evidence could be found. However, in the case of use of Darik's boot and Nuke, all traces of digital evidence were erased (Quick et al., 2013). The work in this research paper has its own limitation since it was performed on a specific cloud storage application on specific operating systems like iOS and Windows.

Chung et al. proposed a new procedure for investigating and analyzing artifacts collected from several devices including Windows and Mac computers as well as Android and iPhone smartphones. The research was conducted on four cloud storage applications: Amazon S3, Dropbox, Evernote and Google Docs accessed via Firefox web browser on the Mac OS X Lion operating system and via Internet Explorer web browser on Windows 7 Vista and XP operating systems. Artifacts on smartphones, iPhone and Android, were also collected for analysis for all four cloud applications. The research lists all the artifacts found on the systems and proves the value of using the procedure in collecting evidence of forensic value (Chung et al., 2012). Nevertheless, the proposed framework should be tested on other cloud storage applications in different environments. The research was conducted in 2012 which implies that the collected artefacts back then may not be found now with newer versions of the applications and operating systems.

Since identifying and collecting digital evidence from electronic devices can be an area of difficulty to forensic practitioners, Choo and Quick determined the location and type of data remnants on a Windows 7 computer and on an iPhone 3G smartphone after a user has undertaken a variety of actions consisting of uploading, downloading and deleting data on Dropbox cloud application. The aim of the research is to determine username, password, software or web browser accessed, files and data remnants and their associated time and date. To gather the data, virtual machines were used to implement the different scenarios with different web browsers including: Internet Explorer, Safari, Mozilla Firefox and Google Chrome, and by installing the Dropbox client software on a computer. Similarly, evidence was collected on an iPhone after using the built-in Safari web browser and downloading the Dropbox mobile application. The Enron dataset was used for this research. It was concluded that there are a wide range of investigation points from where a forensic examiner can collect evidence such as browser history, prefetch files, link files, thumbnails, registry, memory captures, and so on. The location of data and files helped determine the user details and cloud storage information (K. K. R. Choo & Quick, 2013).

Nonetheless, this work does not cover Android smartphones, it is only limited to the iPhone and it covers operating systems that are not widely used anymore.

Teing et al. (2017) conducted a research study about cooperative cloud storage was conducted in order to determine the digital artefact left behind on a user's machine using Symform as a case study. Both mobile devices as well as computers are taken into consideration for the experiment setup. Researchers worked with three operating systems (Windows, Ubuntu and Mac OS) and collected artefacts for each case from three different web browsers (Google Chrome, Internet Explorer and Mozilla Firefox). Additionally, the client software application was downloaded on each of the operating systems mentioned before and on Android KitKat and iOS for smartphones. Network and memory analysis was also conducted for better retrieval of artefacts. The findings of the research show, for each operating system, the location of the sources of evidence and the data artefacts that were found (Sync and file management metadata, authentication and encryption metadata, cloud transaction history and synced files) (Teing et al., 2017). A release of new operating systems and newer versions of applications and hardware may change the recoverability and availability of artifacts on these machines.

Knowing the importance of locating and collecting digital evidence for forensic investigations, Quick and Choo conducted a study on a popular cloud storage application, Google Drive, with the aim of identifying artefacts of forensic value on a computer hard drive running Windows 7 OS and on an Apple iPhone 3G smartphone. Evidence is searched for in memory as well as network traffic. For the forensic analysis performed on Google Drive on a computer hard drive, evidence was recovered from four web browsers (Internet Explorer, Safari, Mozilla Firefox and Google Chrome) and from the client software. In addition, circumstances were created to emulate the case of anti-forensics where a user Eraser or CCleaner to erase Google Drive. The research aimed at collecting username, password, files and their respective time and date. As for the analysis on the iPhone, Google Dive was tested via a web browser built in the smartphone. It was possible to obtain valuable information from locations such as directory listings, prefetch files, link files, thumbnails, registry, browser history, and memory captures. Some of the results acquired were similar to previous research conducted in the field on Microsoft SkyDrive and Dropbox (Quick & Choo, 2014). This research was limited by the fact that the cloud application could not be downloaded on the iPhone. Therefore, it was not possible to test or analyze the application.

For cyber forensic examiners to be informed about the location and sources of evidence on different cloud platforms, a study was conducted on a cloud storage application, pCloud, to determine the different kinds of artefacts retrievable by investigators while examining four popular operating system: Windows, Ubuntu, Android and iOS. Moreover, virtual machines were created to match cases of accessing pCloud through a web browser (Internet Explorer and Google Chrome) on Windows OS and through the installed client software. Network traffic and memory analysis were conducted. The research was concluded with a fair amount of residual artifacts resulting from actions such as install, login, upload, download, uninstall. It was shown that almost all the pCloud credentials were recoverable along with files stored on the cloud (Dargahi et al., 2017). However, this study did not cover anti-forensic techniques and only two kinds of web browsers were used in the process.

"SugarSync forensic analysis" is another study conducted on a cloud storage application to identify and collect data remnants on personal computers and mobile devices running Windows 8, Mac OS X 10.9, Android 4 and iOS 7 devices. The experiments include the set of different activities carried out by a user such as upload and download of files and folders, then document the various digital artefacts that could be recovered from the respective devices. Different virtual machines were created to imitate a user accessing the application either through a web browser (Internet Explorer, Safari, Google Chrome and Mozilla Firefox) or through a client software. Analysis of network traffic and memory were also conducted throughout this research. It was possible to recover important artefacts like username, password, databases, filenames and log files (Shariati et al., 2016). As mentioned in previous research, this study did not present any case of anti-forensics and the work is only specific to one cloud application.

Ubuntu One is another case study for researchers who tried to locate data remnants on different client devices running Windows, Mac and iOS operating systems. For the experiment, virtual machines were used to implement the actions performed by a client on the cloud storage application by accessing it using web browser (Google Chrome, Safari, Mozilla Firefox and Internet Explorer) and through client software. Those experiments were conducted when files were uploaded, downloaded, opened and deleted. Like previous research, memory and network analysis were led. The study provided artifacts of forensic value for practitioners (Shariati et al., 2015). However, the application was not tested on an Android platform.

2.3.3.3 Cloud forensics on mobile phones

After an overview of the research done on cloud storage applications on computers and mobile phones, this section presents only the research done on smartphones.

With the smartphone becoming the primary computing device for many people around the world and the increasing number and importance of cloud storage applications, researchers have developed a cloud focused mobile forensics methodology which aims at collecting and analyzing digital artefacts on a Nexus 4 phone where cloud storage applications (Box, Dropbox, OneDrive and OneNote) were the center of investigation. Researchers were capable of indicating the location of where an application can store data of forensic interest for practitioners including an application's internal storage which usually contains user preferences and database files, an application's external storage and a phone's account data file. The study conducted on Android smartphone provided forensic practitioners with valuable artifacts that do help in facilitating their investigation and accelerating it (Do et al., 2015). Nevertheless, this research was conducted in 2015, a newer version of the OS and applications can affect the amount and location of evidence and the research did not cover Amazon cloud application.

A taxonomy of forensic investigation of cloud storage applications is published to highlight the analysis of artefacts found on 31 cloud storage applications using XRY forensic tool. This taxonomy does assist forensic investigators in future research and in conducting investigations on Android smartphone which aids in correlation of evidence between user activities and remnants of cloud storage applications on the user's device. The Asus Nexus 7 Google tablet was used for the running and analysis of the selected android cloud storage applications and the KitKat 4.4 version of the Android operating system was used. Network traffic was also analyzed using Wireshark and files from the EDRM dataset were chosen to conduct the experiments. While analyzing results, some applications did generate database files and artefacts retrieved from datasets were found in the internal storage included: pictures, documents, audio files and web files. However, in the case of some applications no artefacts were retrieved and in others only database files were generated (Chelihi et al., 2017) . This research contributed greatly to the field of Android forensics, nonetheless, it did not cover Amazon cloud drive application.

A study was conducted on three well known cloud storage applications: Dropbox, Google Drive and OneDrive using the integrated cloud incident handling and forensic by design model. The model was used to determine the artefacts that are likely to remain on an Android device while a user performs a set of actions (e.g., upload, download, share, read, etc.) in different scenarios. These scenarios include using a mobile app with and without an antivirus software and accessing the app via web browser. Analysis of network traffic is also part of the experiment. The study displayed results that varied from user account, user ID, timestamps, files retrieved from cache, file information and size (Hidahya Ab Rahman et al., 2017). The findings indicated that the model is useful for investigations. However, the study did not cover the Amazon cloud application and the model was implemented in a testing environment.

Daryabar et al. offered an up to date view of cloud storage forensics by identifying artefacts that are likely to remain on a client machine running Android and iOS operating system after the user has conducted a set of actions such as uploading, downloading, sharing and deleting files, as well as findings related to the modification of timestamps. Network analysis was also performed in this experiment and MEGA cloud application was used as a case study. The Enron file format dataset was used for the experiment. Findings demonstrated that the content of the files was not modified during the upload and download of files. However, the downloaded files witnessed a change in the timestamps. It was also possible to identify IP and URL addresses of the app, server names and certifications (Daryabar et al., 2017). This research offered a stepping stone for forensic examiners. Yet, it only worked on MEGA cloud app as a case study.

Since mobile devices are highly targeted by cybercriminals, researchers conducted a study with the goal of examining four popular cloud storage applications: OneDrive, Box, Dropbox and Google Drive on two of the most popular operating systems: Android and iOS. Similarly to previous research, the study aims at identifying digital artifacts generated when a user performs actions like downloading, uploading, sharing, logging in and deleting files. Additionally, network analysis was also conducted and the Enron data set was used to conduct the experiments. For each application in every platform and for every action performed, the artefacts were collected, examined and analyzed. The data remnants that were collected included: installation location of the app, username, password, user ID, Timestamp, file name, file content, and file location. The researchers determined that most of the collected evidence is found inside the device's internal memory. Some information was recovered from "info" and "manifest" files, others were found in database files and IP and URL addresses were recovered from network analysis (Dehghantanha et al., 2016). Even though this study offered valuable contributions in the field of mobile cloud forensics, it did not include Amazon Drive application.

Using the evidence collection and analysis methodology for Android devices proposed by Martini et al. (2015), five popular cloud storage applications (Dropbox, OneDrive, , Box and ownCloud), one password sync app (UPM) and two applications for taking notes (OneNote and Evernote) were examined and analyzed on Android devices, in this case using Nexus 4, Galaxy S3 and Android virtual machine. For each application, researchers examined the internal, external storage, the database files and the accounts data of the app using the API. Further analysis conducted on the findings showed that the username and password of the user were recoverable thereby giving the forensic examiners full access to the user's files. Files metadata were stored on the internal storage of the app, offline or cached files were found in the external storage and app configuration files contained data of forensic value (Martini et al., 2015) . Even though the research provided very insightful results about the location and meaning of the artefacts left behind, it did not handle any cases where anti-forensic tools were used. Additionally, the research was conducted in 2015. Newer versions of the application and operating systems are currently available, which means that the same evidence may not be found now.

A study was conducted to determine the residual artifacts that are likely to remain on a mobile device running iOS and Android operating systems. The study aims at answering research questions concerning the type of Meta data that can be recovered from smartphone devices and to which extent the evidence can be recovered in a forensically sound manner and. The study aimed at identifying the effect of downloading, deleting, and uploading files on the extracted data. Tools such as UFED and FTK imager were used to examine and process the devices. Two smartphone devices were used iPhone 3G and HTC desire to emulate the two different operating systems and three cloud storage applications were used for inclusion in this experiment are Dropbox, Box and SugarSync. Researchers used their own predefined data set made of audio, documents, pictures and video files. For the android applications, evidence was recovered from the smartphone itself as well as the SD card and files and metadata were recovered from the device's internal memory. As for the iOS applications, the recovered artifacts were from the internal memory of the device and no deleted files were found and files and Meta data were found in user directory (Grispos et al., 2013) . This research showed that smartphones can provide proxy view of the data stored on the cloud storage service itself. Nonetheless, the work in the study only handled specific applications and it dated back to 2013, so the evidence found back then is considered outdated now and the research did not cover Amazon Cloud application.

A research conducted on mobile devices running Android and iOS operating systems with the aim of showing that end devices do offer a partial view of the evidence stored in the cloud. Researchers used a predefined data set made of videos, documents, audio and pictures and tested them on four different cloud storage applications: Dropbox, Box, SugarSync and Syncplicity. The manipulations performed on the files included: downloading, sharing, deleting and uploading. Also, to create different test scenarios, the manipulations covered different device states including: powered off, cache cleared, active power state, powered off, and cache cleared. Results showed that at some point files were recovered and sometimes deleted files were recoverable as well as thumbnail images and in some cases, certain types of files were recovered more than others (K.-K. R. Choo et al., 2015). With the valuable contributions of this research, it did not expand its work to cover Amazon cloud application.

Table 2.1 Cloud Forensics on Computers

Research Papers	Strengths	Shortcomings
A Case Study On Digital Forensics In The Cloud. (Marturana et al., 2012)	Collected digital evidence of four cloud applications (Flickr, Dropbox, Picasa Web, Google documents) on Internet Explorer, Google Chrome and Mozilla Firefox.	All these research papers are conducted on computers. The findings cannot help forensic investigators in locating evidence on smartphones.
A forensically robust method for acquisition of iCloud data (Oestreicher, 2014)	Collected evidence about iCloud on Mac OS.	
Amazon Cloud Drive forensic analysis (Hale, 2013)	Collected digital evidence of Amazon Cloud application on both Windows 7 and XP	
Cloud Storage Forensic: hubiC as a Case-Study (Blakele et al., 2015)	Collected digital evidence of hubiC cloud application on windows 8.1 on Internet Explorer, Google Chrome and Mozilla Firefox.	
Digital forensic analysis of cloud storage data in IDrive and Mega cloud drive. (Thamburasa et al, 2016)	Collected digital evidence about iDrive and Mega Cloud on Windows 7 using Internet Explorer, Mozilla Firefox and Google Chrome	
Digital forensic evidence collection of cloud storage data for investigation. (Easwaramoorthy et al., 2016)	Collected digital evidence from Amazon Cloud Drive and Microsoft One Drive on Internet Explorer, Google Chrome and Mozilla Firefox running Windows 7.	
Forensic Analysis to China's Cloud Storage Services (Long et al., 2015).	Collected digital evidence from Baidu cloud storage service and 360 on windows 7.	
Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata? (K.-K. R. Choo et al., 2013).	Collected digital evidence from Dropbox, Google Drive and Microsoft Skydrive.	

Table 2.2 Cloud forensics on computers and mobile phones

Research Papers	Strengths	Shortcomings
Cloud Storage Client Application Analysis (Malik et al., 2015).	Collected digital evidence from Copy, ownCloud and Dropbox on Windows 8.1, Android and Ubunutu operating systems.	Some of the following research did not conduct experiments on Android devices. Some of the experiments conducted on Android devices are outdated or did not include enough digital evidence.
Cloud Storage Forensics: ownCloud as a case study (Martini et al., 2013)	Collected digital evidence from ownCloud from Windows and iOS (iPhone) on Internet Explorer, Google Chrome and Mozilla Firefox.	
Digital droplets: Microsoft SkyDrive forensic data remnants (Quick et al., 2013).	Collected digital evidence from Microsoft SkyDrive on Windows 7 (Internet Explorer, Google Chrome, Mozilla Firefox, and Safari) and from iPhone 3G.	
Digital Forensic Investigation of Cloud storage services (Chung et al., 2012).	Collected digital evidence from Amazon S3, Dropbox, Evernote and Google Docs on Windows and Mac computers, in addition to iPhone and Android.	
Dropbox analysis: Data remnants on user machines. (K. K. R. Choo & Quick, 2013).	Collected digital evidence from Dropbox application on iPhone 3G and Windows operating system.	
Forensic Investigation of Cooperative Storage Cloud Service: Symform as a Case Study (Teing et al., 2017).	Collected digital evidence from Symform cloud application on Windows, Ubuntu and Mac OS Android KitKat and iOS.	
Google Drive: Forensic analysis of data remnants (Quick & Choo, 2014).	Collected digital evidence from Google Drive on Windows operating system and iPhone 3G.	
Investigating Storage as a Service Cloud Platform: pCloud as a Case Study (Dargahi et al., 2017).	Collected digital evidence from pCloud on Windows, Mac, Android and iPhone.	
Ubuntu One investigation Detecting evidences on client machine (Shariati et al., 2015).	Collected digital evidence from Ubuntu One on Mac, Windows and iOS.	

SugarSync forensic analysis (Shariati et al., 2016).	Collected digital evidence from SygarSync on Windows, Mac, Android and iPhone.	

Table 2.3 Cloud Forensics on Mobile Forensics

Research Papers	Strengths	Shortcomings
An Android Cloud Storage Apps Forensic Taxonomy (Chelihi et al., 2017)	Collected digital evidence from 31 cloud application on Android devices.	These research papers did not cover Amazon cloud application on Android devices.
A Cloud-Focused Mobile Forensics Methodology (Do et al., 2015).	Collected digital evidence from Box, Dropbox, OneDrive and OneNote on Android devices.	
cloud incident handling and forensic by design: cloud storage as a case study (Hidahya Ab Rahman et al., 2017)	Collected digital evidence from OneDrive, Google Drive and Dropbox on Android devices.	
Cloud storage forensics: MEGA as a case study (Daryabar et al., 2017).	Collected digital evidence form MEGA cloud application on Android and iOS.	
Forensic Investigation of Box, OneDrive, Dropbox and Google Drive applications on Android and iOS devices (Dehghantanha et al., 2016)	Collected digital evidence from OneDrive, Box, Dropbox and Google Drive from Android and iOS.	
Mobile Cloud Forensics: An Analysis of Seven Popular Android Apps (Martini et al., 2015)	Collected digital evidence from Dropbox, OneDrive, Box and ownCloud, OneNote and Evernote on Android devices.	

Using Smartphones as a Proxy for Forensic Evidence Contained in Cloud Storage Services (Grispos et al., 2013)	Collected digital evidence from Dropbox, Box and SugarSync on Android and iOS smartphones.	
Recovering Residual Forensic Data from Smartphone Interactions with Cloud Storage Providers (K.-K. R. Choo et al., 2015)	Collected digital evidence from Dropbox, Box, SugarSync and Synclicity on Android and iOS smartphones.	

2.4 Research Motivation

With the increasing online criminal activity and knowing the value of digital evidence in solving crimes, research in the field of digital forensics is under pressure to always stay up to date. This field has to keep up with the latest electronic devices and the updates performed on software applications and operating systems, which affect the way forensic investigators ought to find, collect, examine, and analyze digital artifacts.

In addition, the field of digital forensics is under researched and there are not enough publications that cover all aspects of cloud mobile forensics which can hinder and slow down the work of the government in criminal and national security investigations.

In a world where everything is moving fast, research in digital forensics saves forensic investigators a lot of time by giving them direct directions on the location of evidence and how to analyze it and by ensuring that no critical evidence is missed during the investigation.

The research conducted in this thesis was conducted on the Amazon cloud application, since this application was downloaded over a million times worldwide and has been overlooked by researchers. So far, this application was not investigated on Android devices and it is unclear as to what type of artefacts it leaves behind and what the access points to assist practitioners are.

The use of cloud storage is increasing among individuals, businesses and governments as a means of storing large amounts of data that can be accessed from mobile devices. However, criminals are taking advantage of this opportunity to hide their traces and their illicit data and make it harder for forensic investigators to identify them.

Therefore, this research was conducted to identify the artifacts left by the Amazon cloud app on an Android smartphone. The aim of this research is to make the work of forensic investigators progress faster and allow them to keep up with the pace of technological advancement.

Chapter 3: Original Work

Chapter 3 is divided into several sections that cover the original work of this thesis. It provides a brief introduction to the overall work, a description of the device's architecture, the forensic framework used, and the experiment setup and research environment. This chapter also covers following investigation phases: evidence source identification and preservation, evidence collection, examination, and analysis and reporting.

3.1 Introduction

The aim of the work presented in this chapter is to answer the research question proposed in Section 1.3 (Research Objectives). The research question enquires about the digital evidence of forensic value that could be found on an Android smartphone after using the Amazon Drive cloud application. The outcome of this research will give investigators a better understanding of the type of evidence and where it might reside on a smartphone, thereby facilitating and speeding up an their work.

Such work was not previously conducted on Amazon's cloud application on a smartphone. Thus, this thesis makes a new addition to the under researched field of digital forensics.

This chapter presents a clear overview of the architecture of the smartphone. It highlights the partitions where evidence might reside. Then, it discusses the forensic framework used throughout the experiment. In addition, it provides a description of the research environment as well as the experiments that were conducted.

This general overview of the work is followed by a detailed description of each stage of the forensic framework. The different steps and actions performed on the device are well defined and the results of the experiments are presented for analysis. Each experiment conducted on the device is properly documented for examination and analysis. Finally, the findings of the investigation are presented.

3.2 Android File Hierarchy

For a good understanding of how the forensic process is applied, it would be useful to have a clear understanding of Android's internal structure. Having knowledge about the structure of the file system and its properties is very helpful for a forensic investigator. To locate forensic evidence, one must understand how Android stores its data in files and folders. Android uses the Linux Kernel and like any other operating system, it is divided into several partitions.

In Linux, the file hierarchy is based on a tree model with the top being called root. As for Android, the file hierarchy is a modified version of the existing Linux hierarchy. The Android operating system organizes the memory into partitions. The following partitions are common:

- /boot: As its name indicates, this partition contains the files needed to boot the smartphone. Without this partition the smartphone cannot boot, since it contains the Kernel and Ramdisk.
- /recovery: This partition allows the user to boot the smartphone into recovery mode to perform advanced recovery and maintenance. This partition is like an alternative boot partition. This partition is also designed for backup purposes.
- /system: This partition contains the whole operating system except the Kernel and Ramdisk, found in the /boot partition. Android user interface and system applications that are pre-installed on the device can be found in this partition.
- /data: This partition is also identified as user data. It holds information specific to user applications. This is where contacts, settings, messages, applications that the user installed can be found. When a factory reset is performed on the device, this partition is wiped. The factory reset restores the device to the state when it was first booted. From a forensic point of view, this partition is highly valuable for investigators, since it contains all the applications' data.
- /cache: This partition stores temporary system data. In other terms, it stores frequently accessed data and some of the logs for fast retrieval. Wiping this

partition does not affect your data. This partition may hold forensically valuable data that may no longer be present in the /data partition.

- /misc: This partition holds information about miscellaneous settings such as hardware settings and USB configuration. It defines the state of the device (on or off).

A forensic investigator's main concern is to locate directories that contain most of the digital evidence. Therefore, it is essential to understand how and where data is stored on the device for a proper extraction. The data provided by the applications is the most valuable. This information can be found in the "/data" partition that holds user application data. The application data resides in the data folder, since Android has a directory structure to store application data. Each application has a subdirectory in the "/data" directory. Each subdirectory has an application "package name", for instance, "com.example.appname". Obviously, this is not the application's user friendly name that is displayed to the user. The application's subdirectory is also known as the application's data directory or private app storage area.

The main focus of a forensic investigator is on the private storage of an application. Android uses sandboxing which prevents applications from interfering and accessing each other's data. In other terms, applications are only allowed to write files to their private storage and other selected places in the external storage. As the private app storage has a limited space, it is preferable for applications to write large files to external storage (physical or emulated SD card). The private app storage can be referred to by internal storage.

Android offers several options to store application data. Applications store data according to its type, size, and whether it should be private or accessible to other applications.

The different locations where data might be stored are:

- Internal file storage stores files that are private to the application and cannot be accessed by other applications. Each application has a private cache directory that stores temporary files. This location is of high forensic value for an investigator.

- External storage stores data that is world readable and can be modified by the user. It is used to store data that is accessible by other applications and saved even after the application is uninstalled. Hence, the external storage does not enforce security measures.

- Shared preferences is where data is stored in key value pairs in a lightweight XML format. Developers can store a wide range of data in "shared_prefs" files that are located in the "shared_prefs" subdirectory of the application's private storage.
- Databases are commonly used by applications to store a range of valuable data such as configuration information, app's metadata or data stored by the user. Android fully supports SQLite databases. Database files usually have a ".db" extension and are stored in the following subdirectory: "/data/data/PackageName/database".

To retrieve the data that can be found in the external storage, internal storage, shared preferences and database files, a forensic investigator needs to follow a forensic framework. The latter specifies the steps and guidelines to conduct an accurate investigation. The forensic framework adopted in this thesis is explained in Section 2.2 (Frameworks and Tools for Extracting Digital Evidence).

The digital forensic framework is composed of four major steps. The first step is evidence identification and preservation, which consists of identifying the device and preserving the evidence. The second step is evidence collection using well defined techniques. The third step is evidence examination and analysis to better understand the meaning of the collected data. And the last step is reporting the results. Each step is conducted in this thesis and explained in details in the following sections.

3.3 Experiment Setup

Having defined the structure of an Android operating system and how it stores data. It is now clear for a forensic investigator where to locate important evidence. To proceed with the work, there should be a clear description of the research in which the experiments will be carried out. This section describes the research environment. This includes an overview of the device, the application, the tools and details about the research environment. Another subsection indicates the dataset that was used as well as the experiments that were conducted on the device.

3.3.1 Research Environment

To set up the research environment for conducting a forensic investigation, it is necessary to state the specification of the device used, the features of the application, the tools and selection criteria.

The smartphone on which the experiments were conducted has the following specifications:

- Device is a Samsung Galaxy SM J500H
- Operating system is Android version 6.0.1
- Internal storage is 8 GB
- Device does not have a memory card

The device was chosen based on practicality and availability at the time when the work was conducted.

The application on which the experiments were carried out is Amazon Drive version 1.9.1.147.0. The application is offered by Amazon Mobile LLC and has more than 1 million downloads. The application offers many features including the following:

- Upload photos, videos, documents and other files from the Android device
- Access the content stored in Amazon Drive, regardless of what device it came from
- Preview photos, videos, PDF, text and Word documents
- Create folders and move files between them
- Search for, rename and delete files and folders
- Download files to the Android device
- Share files as links and attachments through email, text message and other apps

All these features were tested throughout experiments and a forensic investigation was conducted to identify the digital evidence that was produced. This application was chosen since no forensic investigation was conducted on Amazon Drive cloud application.

As for the tools and their selection criteria that were used throughout the work, they are listed as follows:

The computers that were used throughout the experiments were as follows:

- A 64 bit HP computer with an Intel core i7 CPU and 8 GB RAM, running Ubuntu 18.04 LTS operating system was used to collect the forensic image using command line tool.
- A 64 bit HP computer with an Intel core i7 CPU and 4GB RAM running Windows 7 operating system was used to analyze and examine the forensic image.

The tools and the applications that were installed were as follows:

- Odin 3.10.6 is a free tool that can root Samsung device.
- ADB is a command line tool that enable the communication with the device.
- Busybox application is used to provide Linux commands that are not installed by default on Android. In this thesis, the nc (netcat) command is used.
- SuperSu application is an Android utility used to manage root permissions of the installed applications on the device.
- Autopsy version 4.9.0 is an open source digital forensic tool by Basis Technologies that helps in analyzing and examining the forensic image.

These tools were chosen because they are open source, available, and easy to install and use.

3.3.2 Dataset and Experiments

This section in the experiment setup defines the dataset chosen to upload on the cloud application. In addition, it shows how the device was prepared for the experiments and outlines the different experiments that were conducted on the device.

3.3.2.1 Predefined Dataset

The EDRM File Format Dataset was downloaded. It contains 381 files covering 200 file formats. EDRM was chosen because it provides industry standard reference dataset of electronically stored information used for forensic and e-discovery work (EDRM, 2018).

Files from the forensic dataset were chosen to be used in the experiments conducted on the device. Specifically, 8 files of different formats were chosen based on the need to cover the files types that are uploaded to the cloud.

Forensic investigators tend to collect remnants of multimedia files from a suspect's device. Files such as images, videos or audio can contain very sensitive information that could open or close a case in court. In addition, documents hold valuable information that could be used as a proof of evidence in the criminal case. That is why different types of files were selected for the experiments. Since every action performed on a file leaves behind a trace, those files were subjected to different kinds of manipulations. The manipulations varied according to the actions that the cloud application permits such as viewing the picture, deleting a file, playing an audio file, etc. The performed actions are very valuable to forensic investigators to identify key evidence. Table 1 represents all the files that were used in the experiments along with their name, extension, type and manipulations that were performed on them.

Table 3.1 Files Used in the Experiment

ID	File name and extension	File type	File manipulation
1	IMG_1789.jpg	JPEG image	Viewed
2	Michael_Hawley_-_01_-_Sonata_No_21_in_C_Major_Waldstein_Op_53_-_I_Allegro_con_brio.mp3	MP3 format sound	Played
3	Student_Documentation.pdf	PDF file	Shared
4	Disposing-of-Digital-Debris-Information-Governance-Practice-and-Strategy_Page_02.tif	TIFF image	Moved
5	DERM Statistical Data Sample 1.xlsx	Excel worksheet	Renamed
6	Disposing of Digital Debris Sample 1.pptx	Power Point presentation	Downloaded
7	Disposing of Digital Debris – 97.doc	Word document	Uploaded
8	Disposing-of-Digital-Debris.txt	Text document	Moved to trash

3.3.2.2 Experiments

The goal of this study is to identify the data remnants on the device once the user tries to install the application, login, view, play, share, move, rename, download, upload, delete or create a file. In order to achieve this goal, several experiments were prepared and executed on the Android device. Here are the set of activities performed on Amazon Drive cloud application with their IDs:

A1: Login username: laurajsmith799@gmail.com password: *HelloWorld*

A2: View image "IMG_1789.jpg"

A3: Play audio file "Micheal_Hawley_-_01_-_Sonata_No_21_in_C_Major_Waldstein_Op_53_-_ I_Allegro_con_brio.mp3"

A4: Share PDF file "Student_Documentation.pdf" as attachment to vironanouhra@gmail.com

A5: Move TIFF image "Disposing-of-Digital-Debris-Information-Governance-Practice-and-Strategy_Page_02.tif" to Pictures

A6: Rename Excel worksheet "DERM Statistical Data Sample 1.xlsx' to "Data Sample 1"

A7: Download Power Point presentation "Disposing of Digital Debris Sample 1.pptx"

A8: Upload Word document "Disposing of Digital Debris Information Governance Practice and Strategy – 97.doc" to Documents

A9: Move TXT file "Disposing-of-Digital-Debris-Information-Governance-Practice-and-Strategy - Accessible.txt" to trash

A10: Create text file and name it "Sample Text1.txt"

A11: Create a folder and name it "Personal documents" and take a photo of a mouse (AMZ_2018-10-04_15:01:35.jpg) and then upload it

A12: Move to trash the Videos folder

Those experiments were performed on the Android device. Each file was subjected to a different action performed by the user. The actions that were chosen are based on what Amazon Cloud allows its users to do on the application. Those activities provide an investigator with different scenarios to experiment with. The forensic investigator's job is to identify the digital remnants left behind on a smartphone.

3.3.2.3 Device Preparation

In order to conduct the experiments shown in Section 3.3.2.2 (Experiments), it is necessary to prepare the device. This process was broken down into the following stages:

1. The smartphone was reset to the restore the default factory settings. This helps in removing all the previously stored data on the device.
2. The Android smartphone was connected to a wireless internet network to install the Amazon Drive application through the account created on the Playstore. The Playstore account email is laurajsmith799@gmail.com.
3. The cloud application was installed on the device. A new test user account was created using a predefined email and password created specifically for the experiments. The same email was used as the Playstore account (laurajsmith799@gmail.com).
4. A personal computer running Windows 8 was used to access the test account created in step 3 to upload the dataset to Amazon Drive storage using a web browser.
5. The smartphone was synchronized with the Amazon Drive to make sure that the data set was also visible via the Android application.
6. After making sure that the data set was visible on the smartphone, the set of manipulations listed in Experiments were executed.
7. After the experiments were conducted, the device was disconnected from the Internet to avoid any additional changes to the dataset.

   Once the steps are completed, the device enters the cycle of the digital forensic framework for a proper forensic collection of evidence.

3.4 Phases of the Framework

Section 3.4 discusses in details the work done after the experiments were conducted on the device. This section is divided into several steps highlighting the 4 phases of the framework discussed in Section 2.2 (Frameworks and Tools for Extracting Digital Evidence). The phases start with evidence source identification and preservation, then evidence collection followed by examination and analysis of the findings and finally reporting the results. The actions taken in each phase are explained in this section.

3.4.1 Evidence Source Identification and Preservation

This phase is concerned with identifying sources of digital evidence for the forensic investigation. Hence, a forensic investigator should identify the type of the device and approximate the version of the operating system in order to determine the best method to collect the evidence.

However, the practitioner should place the device in a Faraday bag prior to performing any actions. The purpose of a Faraday bag is to create a radio suppressed environment for the device. This will protect the device from being remotely accessed and subjected to any changes in the data over a mobile or WI-FI network. These changes can wipe the internal memory of the device and that should be avoided at all costs. If a Faraday bag is not available, it is recommend to put the device in "Airplane mode" which disables the device's radios.

The device used to conduct the experiments was connected to a private network and was not manipulated by a third party. It was placed in "Airplane mode" to protect it. Since the smartphone was used only as a test device, there were no intentions to damage it. This preserved the digital evidence on the device from being altered.

The device is a Samsung DUOS smartphone as indicated on its back. Therefore a forensic investigator can conclude that the operating system used is Android. By pressing on the home button, the home screen shown indicated that the device ran the Android operating system is Marshmallow version 6. Figure 3.1 below shows the home screen of the device used in the experiments.

Figure 3.1 Samsung SM J500H

3.4.2 Collection of Evidence

This phase is mainly concerned with the collection of digital evidence from the device. This part focuses on extraction techniques and steps followed to acquire the evidence. It is essential to forensic investigators to collect evidence provided by the cloud application Amazon Drive. However, it is physically impossible to seize the servers where the data is stored, in the cloud data center which is located in a different country. A different jurisdiction also leads to lengthy legal procedures to acquire the data found on the cloud. Therefore, a forensic investigator aims at collecting data remnants that are left behind on the Android device. This data will help the practitioner in identifying any valuable information that could help in solving the case much faster.

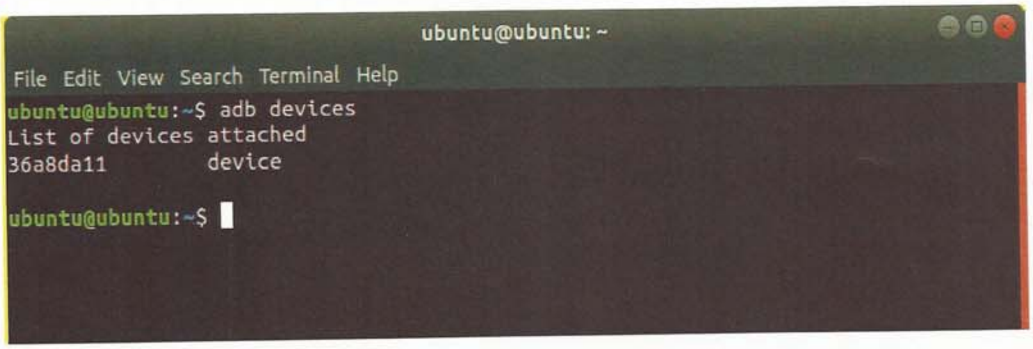
In order to start the phase of evidence collection, the smartphone device will go through three stages. The first stage consists of establishing a connection between the device and the computer. The second stage involves finding an exploit to root the device and gain super user privileges. After ensuring that both the first and second stages were successful, the investigator can issue the imaging command to extract the data.

3.4.2.1 Connecting the device

The first step consists of establishing a connection between the device and the computer. Ubuntu 18.04 LTS is the operating system which the computer runs. Android Studio was installed for the forensic investigator to make use of the Android SDK and the platform tools to establish a connection.

The adb tool will be used to communicate with the device. Adb stands for Android Debug Bridge, is a command line tool which facilitates a variety of actions such as installing and debugging applications. It also gives access to UNIX shell to run commands on the device through the computer.

The adb tool was used with a device connected over USB. Hence, USB debugging and "allow unknown source" options were checked as prerequisites in the smartphone settings. To test whether the device was successfully connected to the computer, *adb devices* command was issued. As shown in Figure 3.2, the command showed the device's serial number and the word "device" which indicates that it is successfully connected.



```
ubuntu@ubuntu:~$ adb devices
List of devices attached
36a8da11        device

ubuntu@ubuntu:~$ 
```

Figure 3.2 ADB command showing the connected device

3.4.2.2 Rooting the device

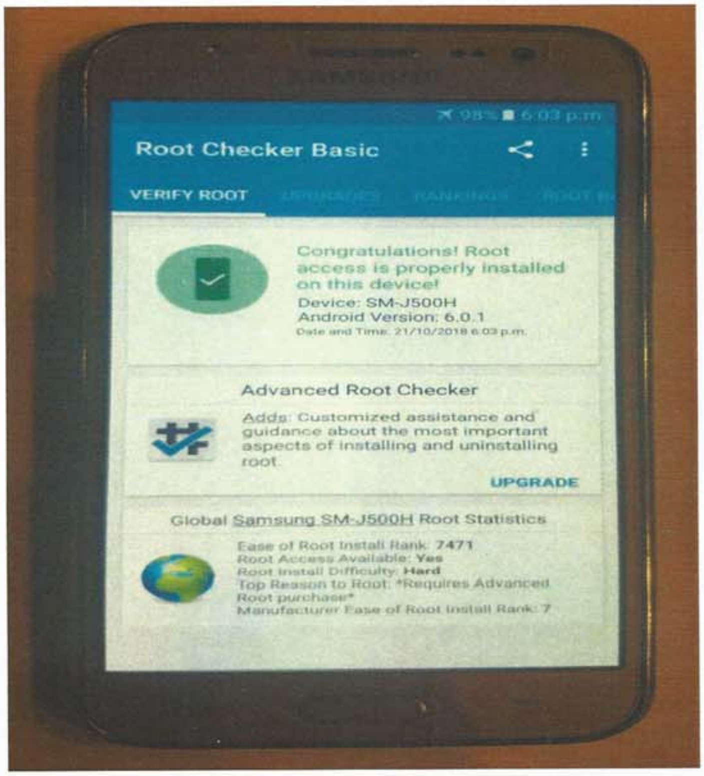
The restrictions imposed by the Android security model prevents the forensic investigator from having full access to the internal storage of the device where the evidence resides. Therefore, rooting is a technique that allows the practitioner to circumvent these restrictions. In the Linux operating system, a "root" user has the power to start or stop any system service, edit or delete any file and many more privileges. These concepts are applied to Android phones, since they are based on Linux. Thus, rooting is required in Android forensics to gain access to the root folder of the Android system where the evidence exists.

In order to perform the rooting process, Samsung Odin version 3.10.6 was installed on the computer. Then, the smartphone was booted into download mode by turning it off, then pressing volume down, power and home buttons and finally pressing the volume up button. Afterwards, the Android smartphone was connected to the computer using a USB cable. The "USB debugging" option was enabled in the smartphone to allow the rooting. The Odin software creates a rooted device for the forensic examiner to access the device's internal storage. Thus, rooting allows a forensic examiner to access files and folders that were not previously accessible with normal user privileges.

Once the Odin software displays PASS this indicates that the device has been successfully rooted. To validate that the phone has been rooted, the root checker APK was installed on the device to check the status of the device. As shown in Figure 3.3, the device has been successfully rooted.

Busybox is a software application which provides some extra Linux commands that are not installed by default on Android. The netcat or nc command is needed in imaging the device and therefore, Busybox is installed on the smartphone. Additionally, superSU APK is also installed on the device. This application provides management of applications that require root access.

Shows *adb –d shell* command issued to start a shell session with the device. This command gives permissions to issue commands directly to the smartphone and interact with it until the shell session is stopped. It is followed by the *su* command which means that all commands run as root until the end of the shell session with the device. To further verify the rooting process, the shell prompt changes from $ sign to # sign upon execution of the *su* command.



Congratulations! Root access is properly installed on this device!
Device: SM-J500H
Android Version: 6.0.1
Date and Time: 21/10/2018 6:03 p.m.

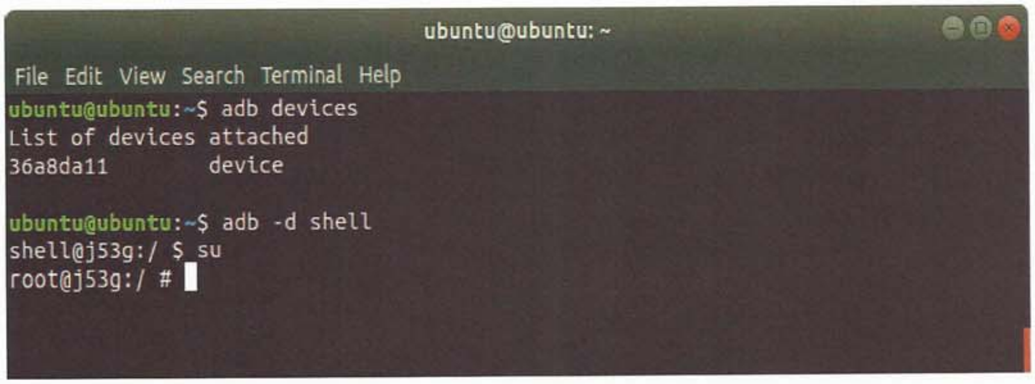
Advanced Root Checker

Adds: Customized assistance and guidance about the most important aspects of installing and uninstalling root.

Global Samsung SM-J500H Root Statistics

Ease of Root Install Rank: 7471
Root Access Available: Yes
Root Install Difficulty: Hard
Top Reason to Root: *Requires Advanced Root purchase*
Manufacturer Ease of Root Install Rank: 7

Figure 3.3 Rooted smartphone



```
ubuntu@ubuntu:~$ adb devices
List of devices attached
36a8da11        device

ubuntu@ubuntu:~$ adb -d shell
shell@j53g:/ $ su
root@j53g:/ #
```

Figure 3.4 Commands to start rooted shell session with the device

3.4.2.3 Imaging the device

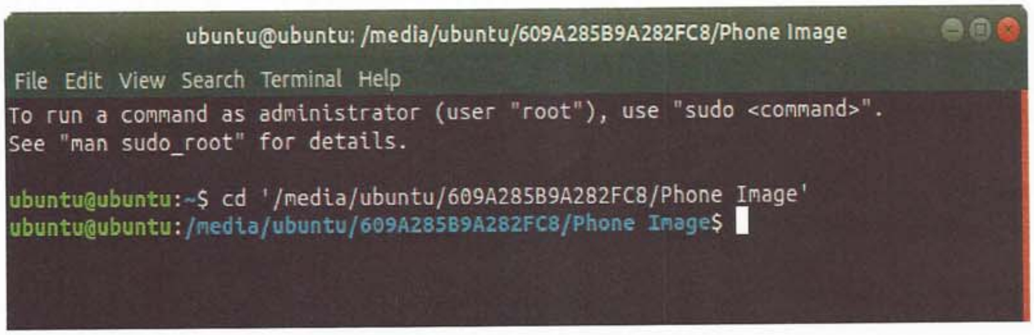
After performing the rooting process of the device and making sure that the smartphone was successfully connected to the computer, it is now time to extract the evidence. Android forensics offers several extraction techniques. Those techniques are previously discussed in Techniques and tools for data extraction.

The process of conducting a physical or logical extraction on the device is called imaging the device. The physical image is ideal for a forensic investigator, since it is a bit by bit image of the Android device memory. This copy contains unallocated space which allows a forensic investigator to collect deleted data. However, the logical acquisition acquires only the data present in the device file system.

To acquire a physical image of the device, the "*dd*" command was used. The acronym "*dd*" stands for data duplicator; it is a built in command line utility used to obtain a raw image of the device's internal storage. Typical command line use of "*dd*" takes if: input file, of: output file. The input file is the data partition of which a bit by bit image will be made and copied onto the output location. The output files is usually a location on the device file system such as the SD card.

The "*dd*" command is used to read blocks from a specified partition and *adb* port forwarding technique with the "*netcat*" utility (computer networking utility for reading from and writing to network connections) is used to write blocks in the case folder on the computer. This strategy is used to avoid using SD cards as a collection target.

Before executing the "*dd*" command, just like the created shell session with the smartphone, there needs to be a shell session for the computer running Linux operating system. Hence, a new terminal is opened and the directory where the device's image will be stored is accessed. Figure 3.5 indicates how cd (change directory) command is used to access the directory where the image will reside.



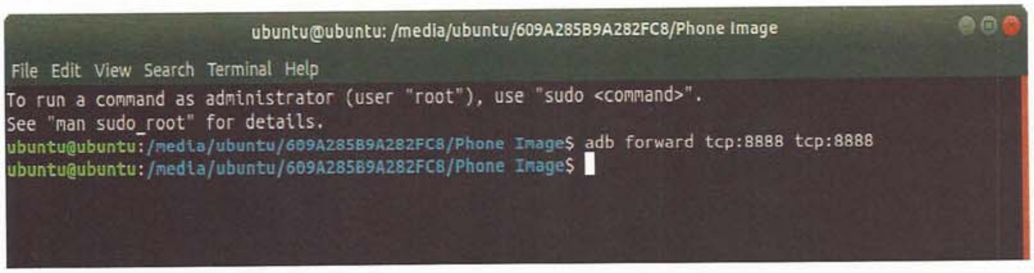
ubuntu@ubuntu: /media/ubuntu/609A285B9A282FC8/Phone Image
File Edit View Search Terminal Help

```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ubuntu:~$ cd '/media/ubuntu/609A285B9A282FC8/Phone Image'
ubuntu@ubuntu:/media/ubuntu/609A285B9A282FC8/Phone Image$
```

Figure 3.5 *cd* command to access directory

Having accessed the directory, using the computer shell, an "*adb*" *forward* command is issued. Figure 3.6 indicates how the forward command is used to allow *adb* to communicate via netcat on port 8888.

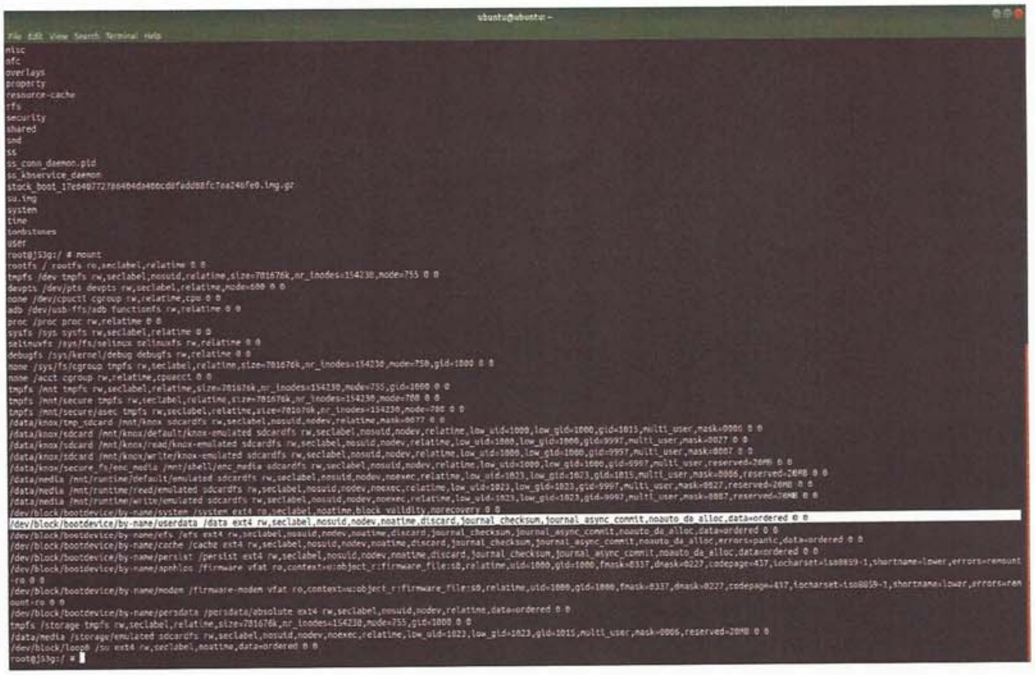


ubuntu@ubuntu: /media/ubuntu/609A285B9A282FC8/Phone Image
File Edit View Search Terminal Help

```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
ubuntu@ubuntu:/media/ubuntu/609A285B9A282FC8/Phone Image$ adb forward tcp:8888 tcp:8888
ubuntu@ubuntu:/media/ubuntu/609A285B9A282FC8/Phone Image$
```

Figure 3.6 abd forward command

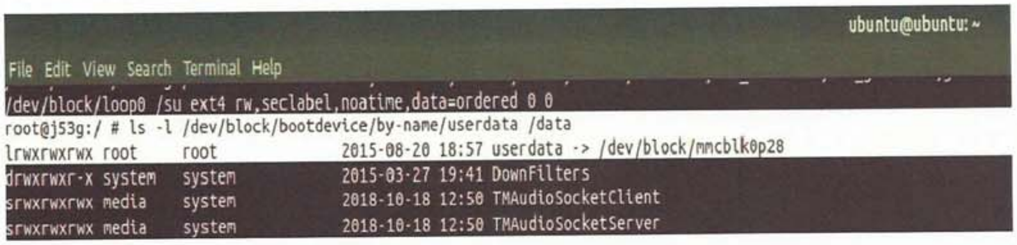
Since the most valuable evidence is found in the "userdata" partition, there is no need to image the entire device. This will save a forensic investigator space as well as time searching in data partitions of no forensic value to the case. To locate the "userdata" partition, a simple mount command on the phone returns the mounted partitions on the device. The "mount" command, executed in phone shell session, will list the different partitions in the device. Hence, allowing the forensic investigator to locate the partitions that need to be imaged. Figure 3.7 Represents the mounted partitions and highlighted in white is the */userdata* partition.



```
misc
nfc
overlays
property
resource-cache
rfs
security
shared
snd
ss
ss_conn_daemon.pid
ss_kbservice_daemon
stock_boot_17e0407727864b4da4bbcd8fadd88fc7ea246fe0.img.gz
su.img
system
time
tombstones
user
root@j53g:/ # mount
rootfs / rootfs ro,seclabel,relatime 0 0
tmpfs /dev tmpfs rw,seclabel,nosuid,relatime,size=781676k,nr_inodes=154230,mode=755 0 0
devpts /dev/pts devpts rw,seclabel,relatime,mode=600 0 0
none /dev/cpuctl cgroup rw,relatime,cpu 0 0
adb /dev/usb-ffs/adb functionfs rw,relatime 0 0
proc /proc proc rw,relatime 0 0
sysfs /sys sysfs rw,seclabel,relatime 0 0
selinuxfs /sys/fs/selinux selinuxfs rw,relatime 0 0
debugfs /sys/kernel/debug debugfs rw,relatime 0 0
none /sys/fs/cgroup tmpfs rw,seclabel,relatime,size=781676k,nr_inodes=154230,mode=750,gid=1000 0 0
none /acct cgroup rw,relatime,cpuacct 0 0
tmpfs /mnt tmpfs rw,seclabel,relatime,size=781676k,nr_inodes=154230,mode=755,gid=1000 0 0
tmpfs /mnt/secure tmpfs rw,seclabel,relatime,size=781676k,nr_inodes=154230,mode=700 0 0
tmpfs /mnt/secure/asec tmpfs rw,seclabel,relatime,size=781676k,nr_inodes=154230,mode=700 0 0
/data/knox/tmp_sdcard /mnt/knox sdcardfs rw,seclabel,nosuid,nodev,relatime,mask=0077 0 0
/data/knox/sdcard /mnt/knox/default/knox-emulated sdcardfs rw,seclabel,nosuid,nodev,relatime,low_uid=1000,low_gid=1000,gid=1015,multi_user,mask=0006 0 0
/data/knox/sdcard /mnt/knox/read/knox-emulated sdcardfs rw,seclabel,nosuid,nodev,relatime,low_uid=1000,low_gid=1000,gid=9997,multi_user,mask=0027 0 0
/data/knox/sdcard /mnt/knox/write/knox-emulated sdcardfs rw,seclabel,nosuid,nodev,relatime,low_uid=1000,low_gid=1000,gid=9997,multi_user,mask=0007 0 0
/data/knox/secure_fs/enc_media /mnt/shell/enc_media sdcardfs rw,seclabel,nosuid,nodev,relatime,low_uid=1000,low_gid=1000,gid=9997,multi_user,reserved=20MB 0 0
/data/media /mnt/runtime/default/emulated sdcardfs rw,seclabel,nosuid,nodev,noexec,relatime,low_uid=1023,low_gid=1023,gid=1015,multi_user,mask=0006,reserved=20MB 0 0
/data/media /mnt/runtime/read/emulated sdcardfs rw,seclabel,nosuid,nodev,noexec,relatime,low_uid=1023,low_gid=1023,gid=9997,multi_user,mask=0027,reserved=20MB 0 0
/data/media /mnt/runtime/write/emulated sdcardfs rw,seclabel,nosuid,nodev,noexec,relatime,low_uid=1023,low_gid=1023,gid=9997,multi_user,mask=0007,reserved=20MB 0 0
/dev/block/bootdevice/by-name/system /system ext4 ro,seclabel,noatime,block_validity,norecovery 0 0
/dev/block/bootdevice/by-name/userdata /data ext4 rw,seclabel,nosuid,nodev,noatime,discard,journal_checksum,journal_async_commit,noauto_da_alloc,data=ordered 0 0
/dev/block/bootdevice/by-name/efs /efs ext4 rw,seclabel,nosuid,nodev,noatime,discard,journal_checksum,journal_async_commit,noauto_da_alloc,data=ordered 0 0
/dev/block/bootdevice/by-name/cache /cache ext4 rw,seclabel,nosuid,nodev,noatime,discard,journal_checksum,journal_async_commit,noauto_da_alloc,errors=panic,data=ordered 0 0
/dev/block/bootdevice/by-name/persist /persist ext4 rw,seclabel,nosuid,nodev,noatime,discard,journal_checksum,journal_async_commit,noauto_da_alloc,data=ordered 0 0
/dev/block/bootdevice/by-name/apnhlos /firmware vfat ro,context=u:object_r:firmware_file:s0,relatime,uid=1000,gid=1000,fmask=0337,dmask=0227,codepage=437,iocharset=iso8859-1,shortname=lower,errors=remount
-ro 0 0
/dev/block/bootdevice/by-name/modem /firmware-modem vfat ro,context=u:object_r:firmware_file:s0,relatime,uid=1000,gid=1000,fmask=0337,dmask=0227,codepage=437,iocharset=iso8859-1,shortname=lower,errors=rem
ount-ro 0 0
/dev/block/bootdevice/by-name/persdata /persdata/absolute ext4 rw,seclabel,nosuid,nodev,relatime,data=ordered 0 0
tmpfs /storage tmpfs rw,seclabel,relatime,size=781676k,nr_inodes=154230,mode=755,gid=1000 0 0
/data/media /storage/emulated sdcardfs rw,seclabel,nosuid,nodev,noexec,relatime,low_uid=1023,low_gid=1023,gid=1015,multi_user,mask=0006,reserved=20MB 0 0
/dev/block/loop0 /su ext4 rw,seclabel,noatime,data=ordered 0 0
root@j53g:/ # 
```

Figure 3.7 /userdata partition

As indicated by Figure 3.7, */dev/block/bootdevice/by-name/userdata/data* is the "userdata" partition where the evidence related to applications can be found. Since writing this directory can be a bit cumbersome. To simplify it, the *ls –l [directory]* command has been issued to get an easier reference for this directory. As shown in Figure 3.8 , the "userdata" directory can be referenced by */dev/block/mmcblk0p28.*

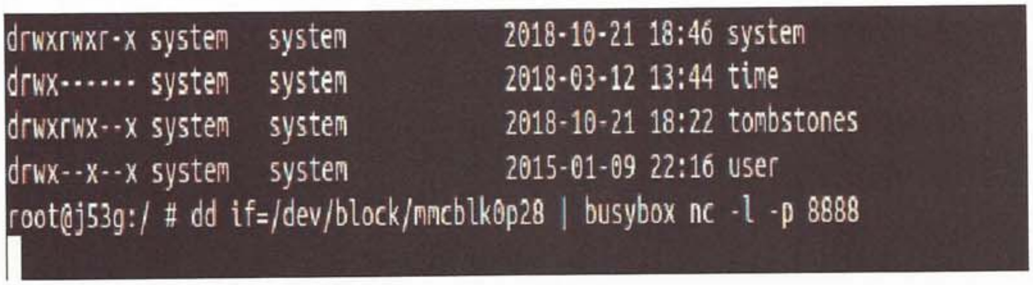


```
/dev/block/loop0 /su ext4 rw,seclabel,noatime,data=ordered 0 0
root@j53g:/ # ls -l /dev/block/bootdevice/by-name/userdata /data
lrwxrwxrwx root     root              2015-08-20 18:57 userdata -> /dev/block/mmcblk0p28
drwxrwxr-x system   system            2015-03-27 19:41 DownFilters
srwxrwxrwx media    system            2018-10-18 12:50 TMAudioSocketClient
srwxrwxrwx media    system            2018-10-18 12:50 TMAudioSocketServer
```

Figure 3.8 userdata partition reference

After identifying the "userdata" partition in the device's shell session and allowing *adb* to communicate via netcat on port 8888 in the computer's shell session. It is possible now to issue the "*dd*" command in the smartphone's shell session to image the "userdata" partition.

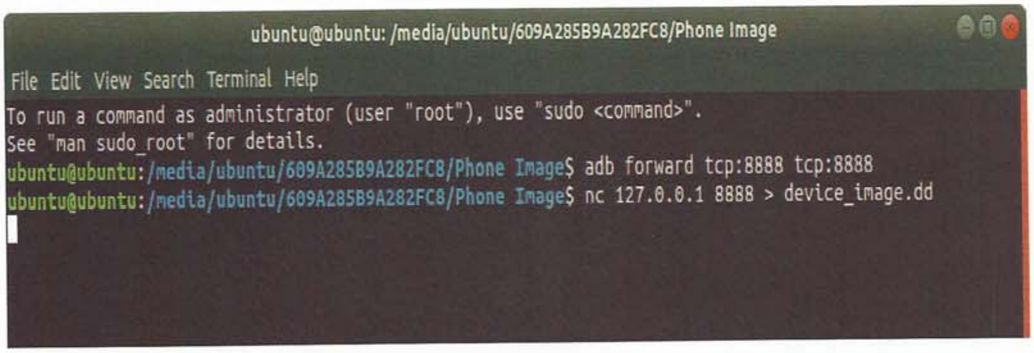
The "*dd*" command reads the content of the "userdata" partition (*/dev/block/mmcblk0p28)* and write it using netcat utility via port 8888 across *adb*. Figure 3.9 shows the "*dd*" command written in the device's shell session.



```
drwxrwxr-x system   system            2018-10-21 18:46 system
drwx------ system   system            2018-03-12 13:44 time
drwxrwx--x system   system            2018-10-21 18:22 tombstones
drwx--x--x system   system            2015-01-09 22:16 user
root@j53g:/ # dd if=/dev/block/mmcblk0p28 | busybox nc -l -p 8888
```

Figure 3.9 dd command

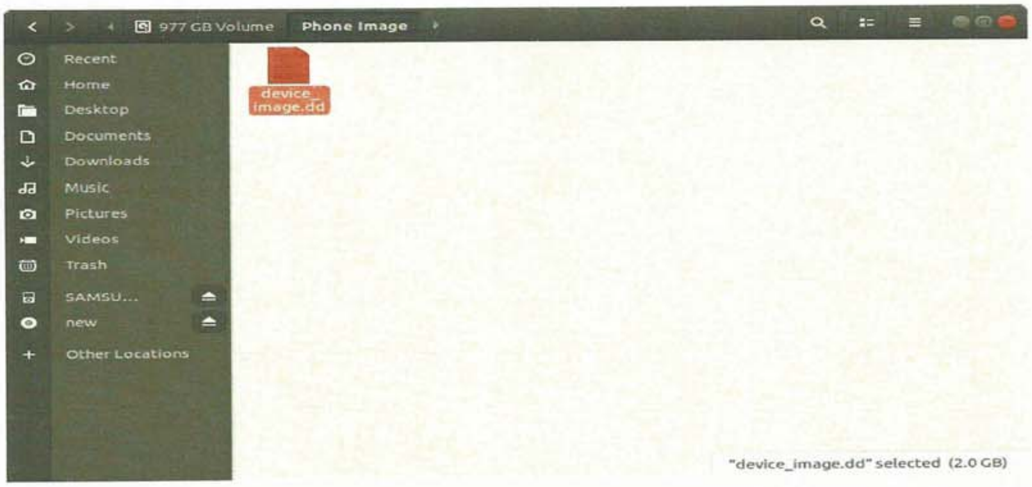
The results of reading the "userdata" partition from the device need to be saved to a file under the name device_image.dd. Therefore, an *nc* command is issued in the computer's shell session to transfer the content of directory across port 8888 to the device_image file. Figure 3.10 Indicates the command used to save the image in the file.


ubuntu@ubuntu: /media/ubuntu/609A285B9A282FC8/Phone Image
File Edit View Search Terminal Help

```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
ubuntu@ubuntu:/media/ubuntu/609A285B9A282FC8/Phone Image$ adb forward tcp:8888 tcp:8888
ubuntu@ubuntu:/media/ubuntu/609A285B9A282FC8/Phone Image$ nc 127.0.0.1 8888 > device_image.dd
```

Figure 3.10 *nc* command

While the content of the directory is being transferred to the file, the window will not allow the examiner to execute any additional commands. At the same time, the size of the file will start to increase gradually. The device_image.dd reached the size of 2GB. Shows the raw image of the "userdata" directory and its size stored on the computer.



"device_image.dd" selected (2.0 GB)

Figure 3.11 Device image

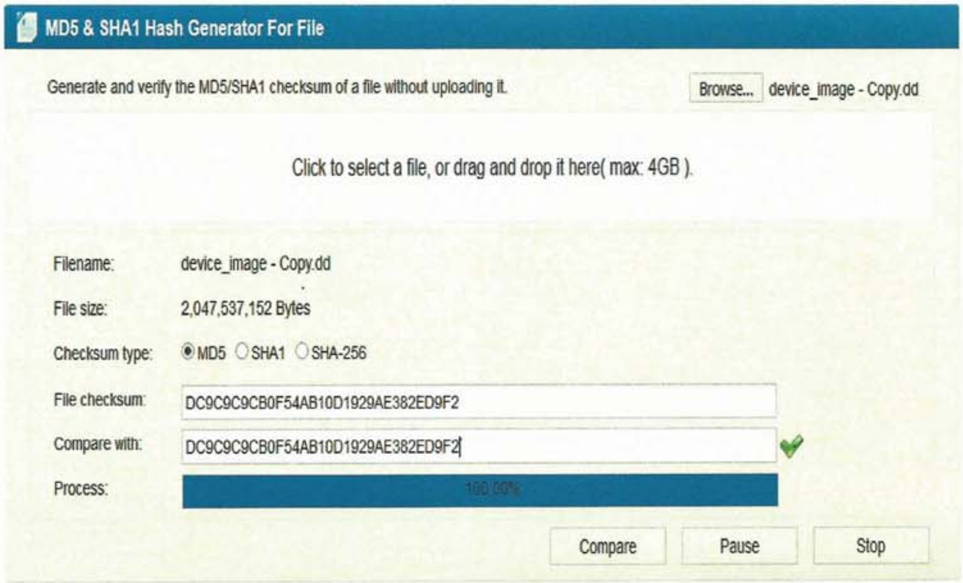
To ensure the practice of proper forensic examination, the raw image collected from the device should be preserved in state that is admissible in court. Any examination should be performed on a copy of the original file and not the original file itself because it might be altered. This method ensures that the evidence presented in court is the same as the original collected.

This is done by creating a hash value of the image. Hash values are computed for both the original and the copy of the file to ensure the integrity of the evidence is maintained. A change in the hash values should be documented and explained. The hash values were computed using md5 hash generator.

The hash value of the original file is: DC9C9C9CB0F54AB10D1929AE382ED9F2.

The hash value of the copy of the original file is:
DC9C9C9CB0F54AB10D1929AE382ED9F2.

Both of these hash values match.



MD5 & SHA1 Hash Generator For File

Generate and verify the MD5/SHA1 checksum of a file without uploading it.

Click to select a file, or drag and drop it here(max: 4GB).

Filename: device_image - Copy.dd

File size: 2,047,537,152 Bytes

Checksum type: ● MD5 ○ SHA1 ○ SHA-256

File checksum: DC9C9C9CB0F54AB10D1929AE382ED9F2

Compare with: DC9C9C9CB0F54AB10D1929AE382ED9F2 ✓

Process: 100.00%

Figure 3.12 Hash value comparison

3.4.3 Examination and Analysis

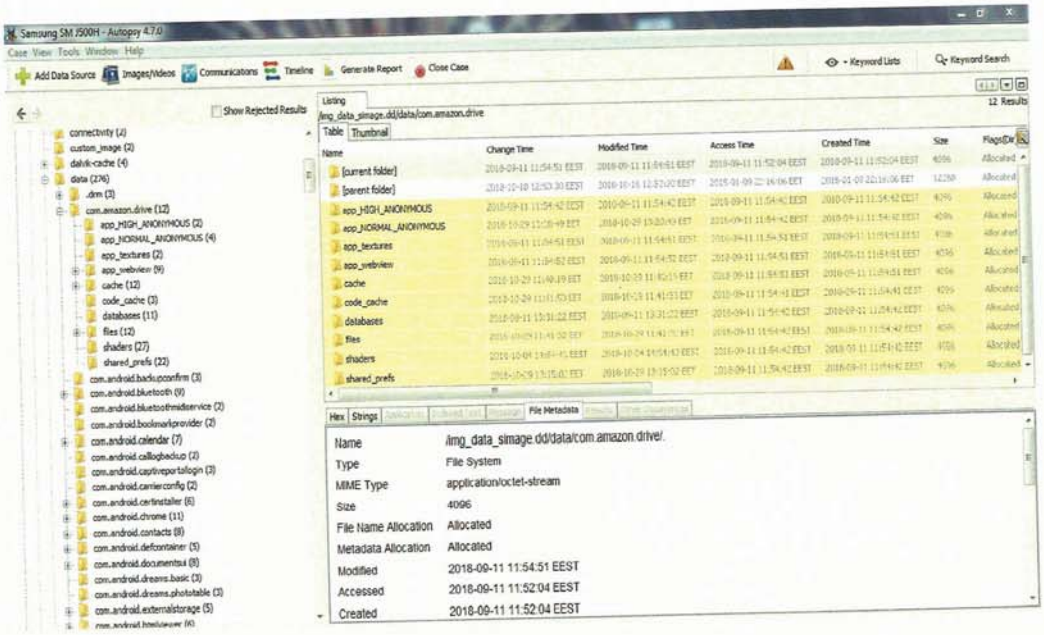
The third phase of the digital forensic framework aims at examining the collected images from the device and analyzing the results. It is very valuable to check whether the analyzed application leaves behind any traces and to locate where and what kind of evidence can be found. This process is essential for forensic investigators since it simplifies and accelerates the investigation. The images are examined and analyzed to identify data remnants.

3.4.3.1 Installation artefacts

From the analysis of forensic image, it was determined that Amazon cloud drive application would be installed as ‘com.amazon.drive’ package in the following path ‘data/data/com.amazon.drive’. It was created on 11/9/2018 at 11:52:04 EEST which is consistent with the actual installation date and time on the device. In addition, in the “accounts.xml” file there were several entries corresponding with the Amazon Drive account.

```
<authority id=”22”id=”0”account=”b269227f-7f14-468b-a7eb-defff4a97c19”
type=”amazon.mixtape.account"authority=”com.amazon.drive.provider.cloud”
syncable=”1”><periosicSync period=”86400”/>
```

This indicates that an account with the user id of 0 and with the account name "b269227f-7f14-468b-a7eb-defff4a97c19" in amazon.mixtape.account of com.amazon.drive.provider.cloud, which is an Amazon Drive authority name. This also indicates that the Amazon account can be synced every 86400 seconds. Additional information related to the Amazon Drive account were found in data/com.amazon/drive/databases/mixtape_accounts.db directory. It included the id of the account "amzn1.account.AF35JUUD5DEOCNYQBAMRVK6D5EDA" (Figure 3.13).



/img_data_simage.dd/data/com.amazon.drive

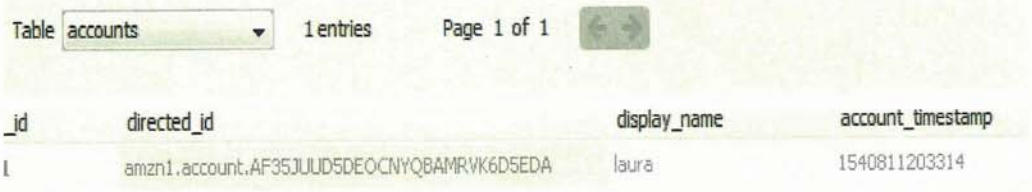
Name	Change Time	Modified Time	Access Time	Created Time	Size	Flags(Dir)
[current folder]	2018-09-11 11:54:51 EEST	2018-09-11 11:54:51 EEST	2018-09-11 11:52:04 EEST	2018-09-11 11:52:04 EEST	4096	Allocated
[parent folder]	2018-10-10 12:53:30 EEST	2018-10-16 12:52:20 EEST	2015-01-09 22:16:06 EET	2015-01-09 22:16:06 EET	12288	Allocated
app_HIGH_ANONYMOUS	2018-09-11 11:54:42 EEST	2018-09-11 11:54:42 EEST	2018-09-11 11:54:42 EEST	2018-09-11 11:54:42 EEST	4096	Allocated
app_NORMAL_ANONYMOUS	2018-10-29 13:20:49 EET	2018-10-29 13:20:49 EET	2018-09-11 11:54:42 EEST	2018-09-11 11:54:42 EEST	4096	Allocated
app_textures	[illegible]	[illegible]	[illegible]	[illegible]	4096	Allocated
app_webview	2018-09-11 11:54:52 EEST	2018-09-11 11:54:52 EEST	2018-09-11 11:54:51 EEST	2018-09-11 11:54:51 EEST	4096	Allocated
cache	2018-10-29 11:40:19 EET	[illegible]	[illegible]	[illegible]	4096	Allocated
code_cache	2018-10-29 11:41:53 EET	2018-10-29 11:41:53 EET	2018-09-11 11:54:41 EEST	2018-09-11 11:54:41 EEST	4096	Allocated
databases	2018-09-11 13:31:22 EEST	2018-09-11 13:31:22 EEST	2018-09-11 11:54:42 EEST	2018-09-11 11:54:42 EEST	4096	Allocated
files	[illegible]	[illegible]	2018-09-11 11:54:42 EEST	2018-09-11 11:54:42 EEST	4096	Allocated
shaders	[illegible]	[illegible]	2018-09-11 11:54:42 EEST	[illegible]	4096	Allocated
shared_prefs	[illegible]	[illegible]	2018-09-11 11:54:42 EEST	[illegible]	4096	Allocated

Name	/img_data_simage.dd/data/com.amazon.drive/.
Type	File System
MIME Type	application/octet-stream
Size	4096
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2018-09-11 11:54:51 EEST
Accessed	2018-09-11 11:52:04 EEST
Created	2018-09-11 11:52:04 EEST

Figure 3.13 com.amazon.drive package

3.4.3.2 Login analysis

During the analysis of the forensic image of the device to find artefacts related to the Amazon Drive account, the username and the password of the account were not found. However, it was possible to find, in /data/com.amazon.drive/databases directory, the map_data_storage.db database file that contained the first name of the account user "laura" and the last time when the user was active in Epoch time: 1540811203314 (Monday, October 29, 2018 1:06:43.314 PM in EET). In addition to the ID of the account amzn1.account.AF35JUUD5DEOCNYQBAMRVK6D5EDA (Figure 3.14).



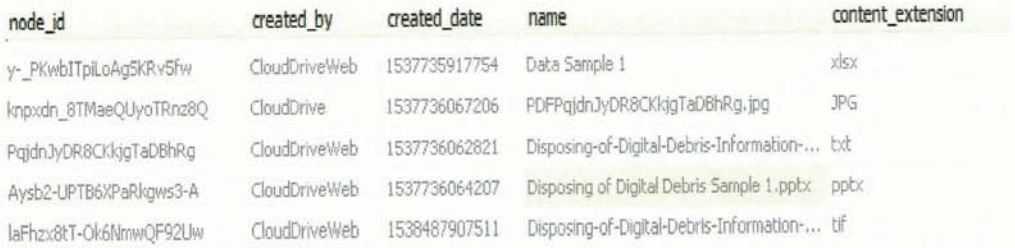
_id	directed_id	display_name	account_timestamp
1	amzn1.account.AF35JUUD5DEOCNYQBAMRVK6D5EDA	laura	1540811203314

Figure 3.14 Amazon Drive account

3.4.3.3 Download analysis

An analysis of the collected forensic image was conducted to determine the artefacts left behind after the user tries to download a file. In this case, the downloaded file was a Power Point presentation according to activity A7 in Experiments.

At first, the file was located in the database of the Amazon Drive account (amzn1.account.AF35JUUD5DEOCNYQBAMRVK6D5EDA.mixtape.db) in the following directory: /data/com.amazon.drive/databases (Figure 3.15). After further search, it was also possible to find the downloaded Power Point file in the "/media/0/Download" directory. The file is called "Disposing of Digital Debris Sample1.pptx" and was created on September 23, 2018 at 11:54:24 EEST (1537736064207 in Epoch time) by CloudDriveWeb. This means that the file was first uploaded on the account using the web and not the mobile application. The status id of the file is 1, which means that the file is available. It was possible to retrieve the content of the file (text only) and determine that the file was downloaded on October 4 2018 at 14:55:46 EEST.

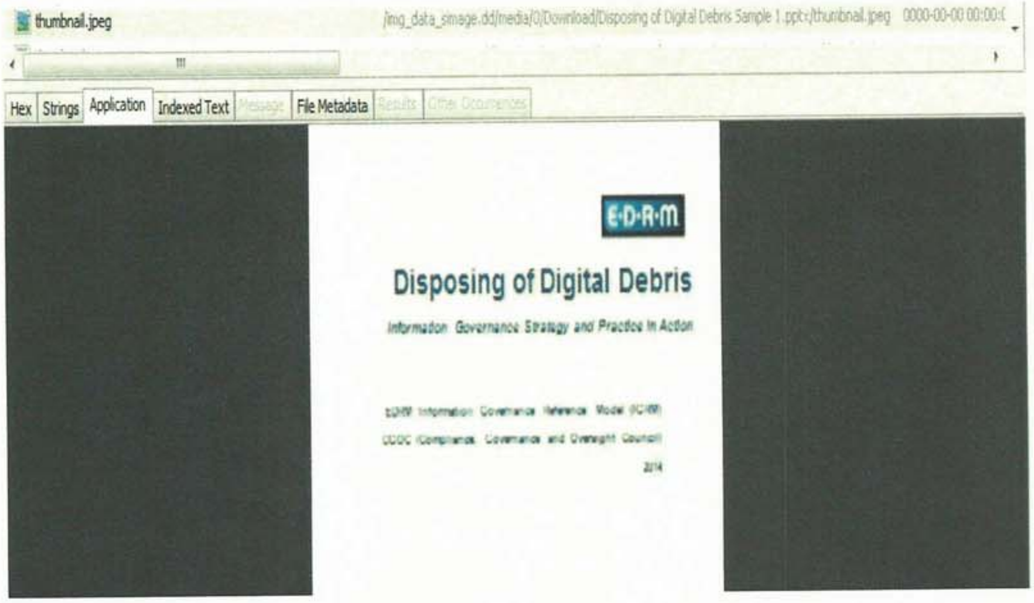


node_id	created_by	created_date	name	content_extension
y-_PKwbITpiLoAg5KRv5fw	CloudDriveWeb	1537735917754	Data Sample 1	xlsx
knpxdn_8TMaeQUyoTRnz8Q	CloudDrive	1537736067206	PDFPqjdnJyDR8CKkjgTaDBhRg.jpg	JPG
PqjdnJyDR8CKkjgTaDBhRg	CloudDriveWeb	1537736062821	Disposing-of-Digital-Debris-Information-...	txt
Aysb2-UPTB6XPaRkgws3-A	CloudDriveWeb	1537736064207	Disposing of Digital Debris Sample 1.pptx	pptx
laFhzx8tT-Ok6NmwQF92Uw	CloudDriveWeb	1538487907511	Disposing-of-Digital-Debris-Information-...	tif

Figure 3.15 Disposing of Digital Debris Sample 1.pptx in database

It is interesting to note that the first slide of the power point presentation was found stored under the name "thumbnail.jpeg" under the following path: "/media/0/Download/ Disposing of Digital Debris Sample1.pptx/thumbnail.jpeg".

Additional information were found about the author of the file "tzhuang" and the creation date of the file "25 November 2014".


thumbnail.jpeg /img_data_image.dd/media/0/Download/Disposing of Digital Debris Sample 1.pptx/thumbnail.jpeg 0000-00-00 00:00:(

E·D·R·M

Disposing of Digital Debris

Information Governance Strategy and Practice in Action

EDRM Information Governance Reference Model (IGRM)

CGOC (Compliance, Governance and Oversight Council)

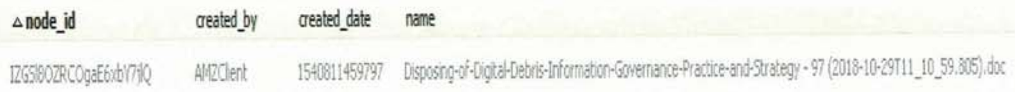
2014

Figure 3.16 Slide 1 of Power Point file

3.4.3.4 Upload analysis

In this section, an analysis was conducted on the forensic image to locate evidence related to the upload process of a file. In this case, the uploaded file was a Word document according to activity A8 in Experiments.

At first, the file was located in the database of the Amazon Drive account (amzn1.account.AF35JUUD5DEOCNYQBAMRVK6D5EDA.mixtape.db) in the following directory: "/data/com.amazon.drive/databases" (Figure 3.17). The file name is "Disposing of Digital Debris Information Governance Practice and Strategy-97.doc". It was created on October 29, 2018 at 1:10:59 EEST (15408114599797 in Epoch time) by AMZClient. This means that the user has uploaded the file manually on the mobile application. The status id of the file is 1 which indicates that the file is available. The file's node id is "IZGSI8OZRCOgaE6XBy7jIQ", with a parent node id of "Z5Zfg4yqt2pYgb8JX2Brw". The latter id is the id of the Documents folder. This means that the file was uploaded to the Documents folder.



△ node_id	created_by	created_date	name
IZGSI8OZRCOgaE6xbY7jIQ	AMZClient	1540811459797	Disposing-of-Digital-Debris-Information-Governance-Practice-and-Strategy - 97 (2018-10-29T11_10_59.305).doc

Figure 3.17 Disposing of Digital Debris Information Governance Practice and Strategy 97

After further analysis, the file was found in "media/0/download" directory, since after uploading the file it was opened in the application. The content of the file was extracted, the text along with the image found in the document. The image was found under the following path: "/media/0/Download/Disposing-of-Digital-Debris-Information-Governance-Practice-and-Strategy-97.doc/0.png" (Figure 3.18).

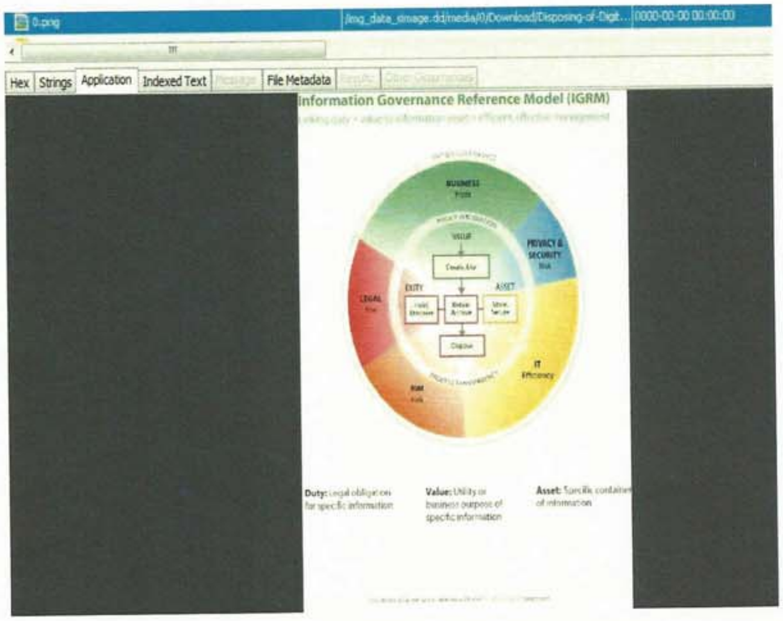
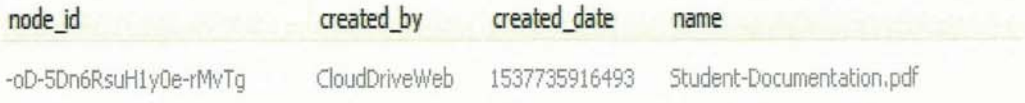

0.png
/img_data_image.dd/media/0/Download/Disposing-of-Digit...
0000-00-00 00:00:00
Hex
Strings
Application
Indexed Text
File Metadata
Information Governance Reference Model (IGRM)
BUSINESS
PRIVACY & SECURITY
VALUE
DUTY
ASSET
LEGAL
IT
Efficiency
Dispose
Duty: Legal obligation for specific information
Value: Utility or business purpose of specific information
Asset: Specific container of information

Figure 3.18 Image retrieved from the uploaded file

3.4.3.5 Share analysis

In this section, an analysis was conducted on the forensic image to identify evidence of forensic value when a file is shared as an attachment and sent via email. In this case, the shared file is a pdf document sent as an attachment to vironanouhra@gmail.com according to activity A4 in Experiments.

At first, the file was found in the database of the Amazon Drive account (amzn1.account.AF35JUUD5DEOCNYQBAMRVK6D5EDA.mixtape.db) in the following directory: "/data/com.amazon.drive/databases" (Figure 3.19). The file name is "Student-Documentation.pdf". The file was created on September 23, 2018 at 11:51:56 EEST (1537735916493 in Epoch time) by CloudDriveWeb, which means that the file was added to the account using the web and not the mobile application. The status id of the file is 1 which means that the file is available.



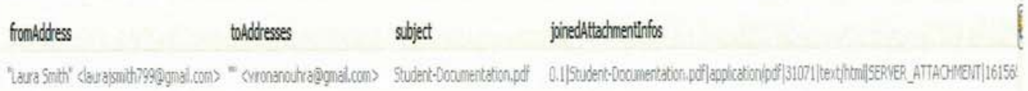
node_id	created_by	created_date	name
-oD-5Dn6RsuH1y0e-rMvTg	CloudDriveWeb	1537735916493	Student-Documentation.pdf

Figure 3.19 Student Documentation PDF

After additional research, the file was also found in the following directory: "/data/com.amazon.drive/cache/original/-oD5Dn6RsuH1y0erMvTg/777cac9d7f6c130f921b1a461dec8031". It was possible to extract the file's content (text), its author (htgilbert), as well as its creation date (23rd of October 2009).

In addition, valuable artefacts were found in the following file: "data/com.google.android.gm/databases/mailestore.laurajsmith799@gmail.com.db". The conversation was sent from address "Laura Smith" laurajsmith799@gmail.com to address vironanouhra@gmail.com with the following subject: "Student-Documentation.pdf". This finding indicates that the email laurajsmith799@gmail.com is used to access the Amazon Drive account. Additionally, the date the message was sent and received were shown in Epoch time, October 4, 2018 at 2:53:07 (1538653987000) and October 4, 2018 at

2:53:07:162, (1538653987164) respectively. Furthermore, the attachment information showed the "Student-Documentation.pdf" file (Figure 3.20).



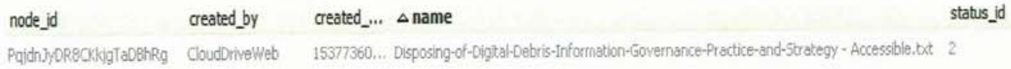
fromAddress	toAddresses	subject	joinedAttachmentInfos
"Laura Smith" <laurajsmith799@gmail.com>	"" <vironanouhra@gmail.com>	Student-Documentation.pdf	0.1|Student-Documentation.pdf|application/pdf|31071|text/html|SERVER_ATTACHMENT|16156

Figure 3.20 Student documentation attachment

3.4.3.6 Delete analysis

This section reports on an analysis that was conducted to locate any evidence of forensic value that might help the investigator when a user moves a file and a folder to the trash. In activity A9 the user moved the following file to the trash: "Disposing-of-Digital-Debris-Information-Governance-Practice-and-Strategy - Accessible.txt". In activity A12 the user moved the videos folder to trash.

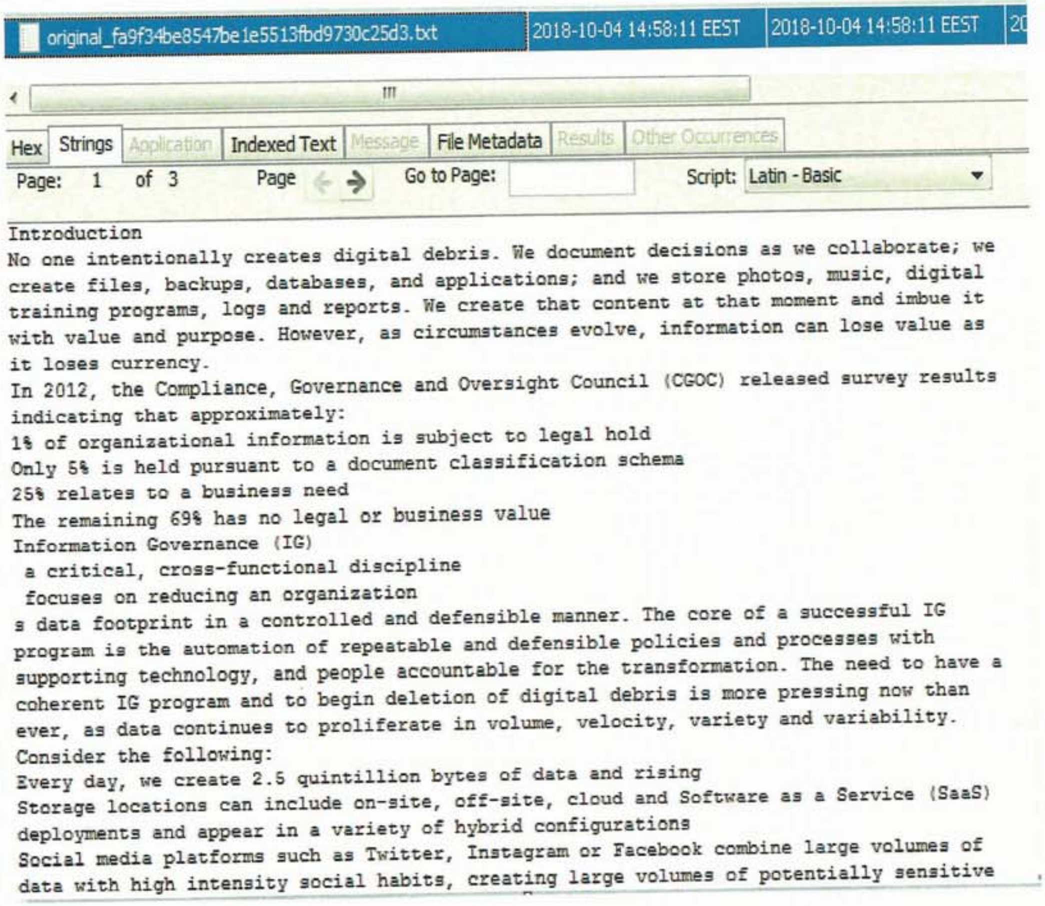
While conducting the analysis, a file called "Disposing-of-Digital-Debris-Information-Governance-Practice-and-Strategy - Accessible.txt" was found in the database of the Amazon account (amzn1.account.AF35JUUD5DEOCNYQBAMRVK6D5EDA.mixtape.db) in the "/data/com.amazon.drive/databases" directory (Figure 3.21). The file was created on September 23, 2018 at 23:54:22 EEST (1537736062821 in Epoch time) by CloudDriveWeb. The file was then deleted on October 4, 2018 at 14:58:18 EEST (1540811574847 in Epoch time). The status id of the file is 2, which means that the file is trashed.



node_id	created_by	created_...	△ name	status_id
PqjdnJyDR8CKkjgTaDBhRg	CloudDriveWeb	15377360...	Disposing-of-Digital-Debris-Information-Governance-Practice-and-Strategy - Accessible.txt	2

Figure 3.21 Disposing-of-Digital-Debris-Information-Governance-Practice-and-Strategy - Accessible.txt

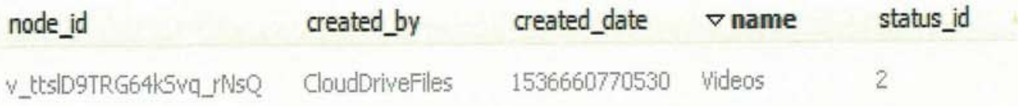
Even though the file was deleted, the file was found in the "/data/com.amazon.drive/cache/P/PqjdnJyDR8CKkjgTaDBhRg" directory using the md5 hash of the file (fa9f34be8547be1e5513fbd9730c25d). The file was found under another name "original_fa9f34be8547be1e5513fbd9730c25d3.txt". It was also possible to retrieve the content of the file (text) (Figure 3.22).



```
Introduction
No one intentionally creates digital debris. We document decisions as we collaborate; we
create files, backups, databases, and applications; and we store photos, music, digital
training programs, logs and reports. We create that content at that moment and imbue it
with value and purpose. However, as circumstances evolve, information can lose value as
it loses currency.
In 2012, the Compliance, Governance and Oversight Council (CGOC) released survey results
indicating that approximately:
1% of organizational information is subject to legal hold
Only 5% is held pursuant to a document classification schema
25% relates to a business need
The remaining 69% has no legal or business value
Information Governance (IG)
 a critical, cross-functional discipline
 focuses on reducing an organization
s data footprint in a controlled and defensible manner. The core of a successful IG
program is the automation of repeatable and defensible policies and processes with
supporting technology, and people accountable for the transformation. The need to have a
coherent IG program and to begin deletion of digital debris is more pressing now than
ever, as data continues to proliferate in volume, velocity, variety and variability.
Consider the following:
Every day, we create 2.5 quintillion bytes of data and rising
Storage locations can include on-site, off-site, cloud and Software as a Service (SaaS)
deployments and appear in a variety of hybrid configurations
Social media platforms such as Twitter, Instagram or Facebook combine large volumes of
data with high intensity social habits, creating large volumes of potentially sensitive
```

Figure 3.22 Content of deleted file

The Videos folder is found by default in the Amazon Drive account with the Pictures and Documents folder when a user creates a new account. In A12 the folder was deleted. However, it was possible to locate the folder in the database file (amzn1.account.AF35JUUD5DEOCNYQBAMRVK6D5EDA.mixtape.db) of the Amazon Drive account. The folder was created on the 11th of September 2018 at 13:12:50 EEST (1536660770530 in Epoch time) by CloudDriveFiles. The kind id of the file is 1 which means it is a folder. The status id of the folder is 2 which means that the folder is in the trash. The folder was deleted on October 4, 2018 at 3:00:20 EEST (1538654420370 in Epoch time.



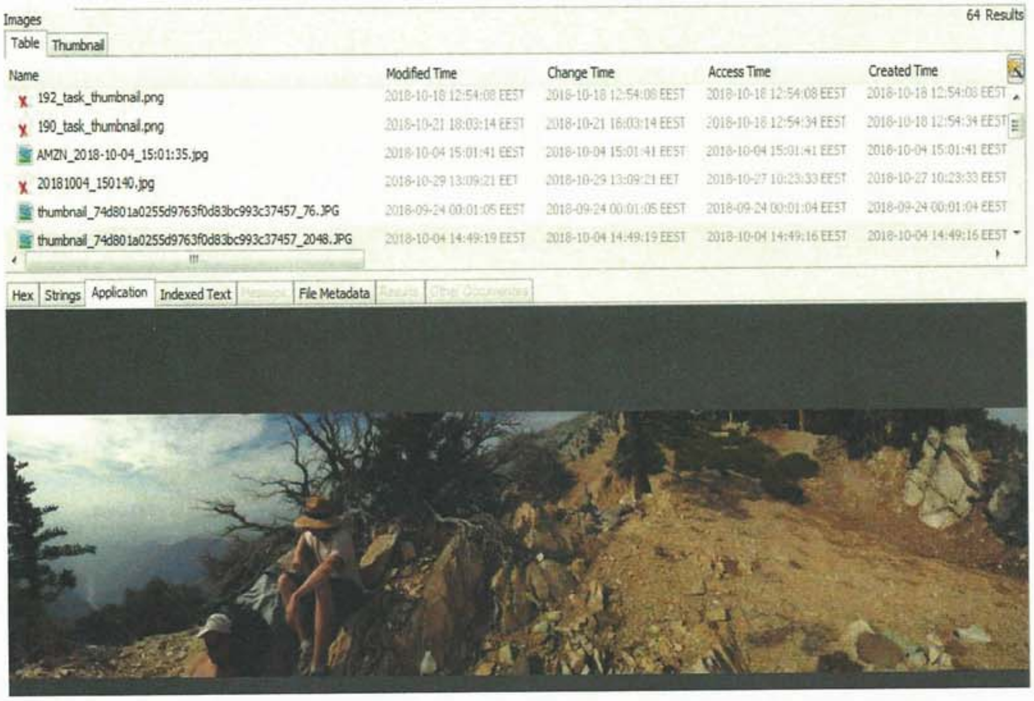
node_id	created_by	created_date	▽ name	status_id
v_ttslD9TRG64kSvq_rNsQ	CloudDriveFiles	1536660770530	Videos	2

Figure 3.23 Videos folder

3.4.3.7 Additional analysis

In this section, analysis was conducted to find the evidence of forensic value that can be found on the phone when the other activities were conducted. The activities are A2: viewing an image "IMG_1789.JPG". A3: playing and audio file. A5: moving a TIFF image to Pictures folder. A6: renaming an excel worksheet to "Data sample 1". A10: creating a text file "Sample Text1.txt". A11: creating a folder, naming it "personal documents" and taking a photo and uploading it.

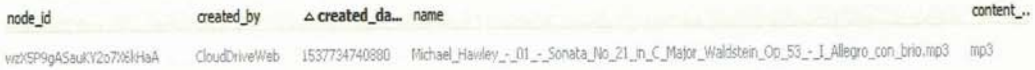
Regarding A2 (view image), the "IMG_1789.JPG" was found in the database file of the Amazon Drive account (amzn1.account.AF35JUUD5DEOCNYQBAMRVK6D5EDA.mixtape.db). The image was created on September 23rd, 2018 at 23:16:01 EEST (1537733761413 in Epoch time) by CloudDriveWeb. The image was viewed on the 4th of October, 2018 at 14:49:19 EEST. The image status id is 1, this indicates that the file is available. After additional research, it was possible to locate the image in the following directory "/data/com.amazon.drive/cache/t/toV7UWi3SICcILdFYYWwyQ" under the following name "thumbnail_74d801a0255d9763f0d83bc993c37457_2048.JPG". The actual image was extracted, even though it was not downloaded on the device (Figure 3.24).



Name	Modified Time	Change Time	Access Time	Created Time
192_task_thumbnail.png	2018-10-18 12:54:08 EEST	2018-10-18 12:54:08 EEST	2018-10-18 12:54:08 EEST	2018-10-18 12:54:08 EEST
190_task_thumbnail.png	2018-10-21 18:03:14 EEST	2018-10-21 18:03:14 EEST	2018-10-18 12:54:34 EEST	2018-10-18 12:54:34 EEST
AMZN_2018-10-04_15:01:35.jpg	2018-10-04 15:01:41 EEST	2018-10-04 15:01:41 EEST	2018-10-04 15:01:41 EEST	2018-10-04 15:01:41 EEST
20181004_150140.jpg	2018-10-29 13:09:21 EET	2018-10-29 13:09:21 EET	2018-10-27 10:23:33 EEST	2018-10-27 10:23:33 EEST
thumbnail_74d801a0255d9763f0d83bc993c37457_76.JPG	2018-09-24 00:01:05 EEST	2018-09-24 00:01:05 EEST	2018-09-24 00:01:04 EEST	2018-09-24 00:01:04 EEST
thumbnail_74d801a0255d9763f0d83bc993c37457_2048.JPG	2018-10-04 14:49:19 EEST	2018-10-04 14:49:19 EEST	2018-10-04 14:49:16 EEST	2018-10-04 14:49:16 EEST

Figure 3.24 IMG_1789.JPG

Regarding A3 (play audio), the "Michael_Hawley_-_01_-_Sonata_No_21_in_C_Major_Waldstein_Op_53_-_I_Allegro_con_brio.mp3" file was found in the database file of the Amazon Drive account (amzn1.account.AF35JUUD5DEOCNYQBAMRVK6D5EDA.mixtape.db) (Figure 3.25).

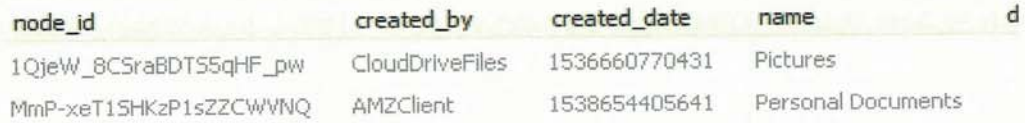


node_id	created_by	△created_da...	name	content_..
wzXSP9gASauKY2o7X6kHaA	CloudDriveWeb	1537734740880	Michael_Hawley_-_01_-_Sonata_No_21_in_C_Major_Waldstein_Op_53_-_I_Allegro_con_brio.mp3	mp3

Figure 3.25 Audio file

The audio file was created on September 23, 2018 at 23:32:20 EEST (1537734740880 in Epoch time) by CloudDriveWeb. The audio file status id is 1, this indicates that the file is available. However, it was not possible to extract the audio file nor determine when it was listened to.

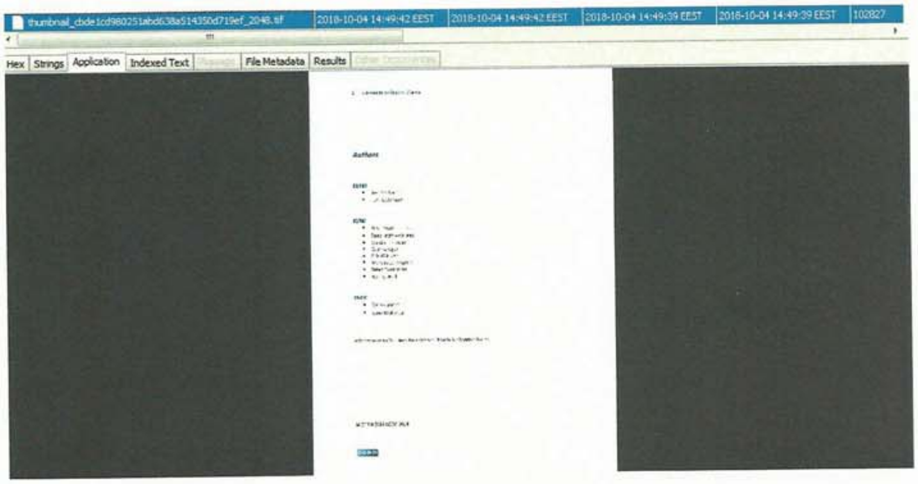
Regarding A5 (move image), the TIFF image (Disposing-of-Digital-Debris-Information-Governance-Practice-and-Strategy_Page_02.tif) was found in file was found in the database file of the Amazon Drive account (amzn1.account.AF35JUUD5DEOCNYQBAMRVK6D5EDA.mixtape. db). It was created by CloudDriveWeb on October 4, 2018 at 14:54:06 EEST (1538654046308 in Epoch time) with a node id of "laFhzx8tT-Ok6NmwQF92Uw". With additional research, it was possible to determine the parent node id of the TIFF image which is "1QjeW_8CSraBTDS5qHF_pw". The parent node id refers to the Pictures folder created by the CloudDriveFiles (Figure 3.26). This means that the TIFF image is in the Pictures folder.



node_id	created_by	created_date	name	d
1QjeW_8CSraBDTS5qHF_pw	CloudDriveFiles	1536660770431	Pictures	
MmP-xeT1SHKzP1sZZCWVNQ	AMZClient	1538654405641	Personal Documents	

Figure 3.26 Node id of Pictures folder

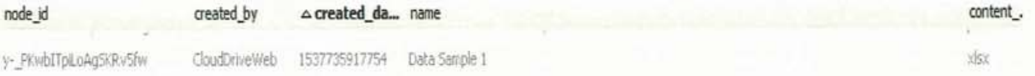
Furthermore, the TIFF image was extracted. It was located, using md5 hash value of the file content, in the "/data/com.amazon.drive/cache/I/laFhzx8tT-Ok6NmwQF92Uw" directory under the name "thumbnail_cbde1cd980251abd638a514350d719ef_2048.tif" (Figure 3.27).



thumbnail_cbde1cd980251abd638a514350d719ef_2048.tif	2018-10-04 14:49:42 EEST	2018-10-04 14:49:42 EEST	2018-10-04 14:49:39 EEST	2018-10-04 14:49:39 EEST	102827

Figure 3.27 TIFF image

Regarding A6 (rename file), the "Data Sample 1" file was found in file was found in the database file of the Amazon Drive account (amzn1.account.AF35JUUD5DEOCNYQBAMRVK6D5EDA. mixtape.db) (Figure 3.28). It was created by CloudDriveWeb on September 23, 2018 at 23:51:57 EEST (1537735917754 in Epoch time). It was possible to find the file in the "/data/com.amazon.drive/y/y-_PKwbITpiLoAgSKRv5fw" directory under the following name "original_9005d6f1951b557022cbbd99180edadc.xlxs".

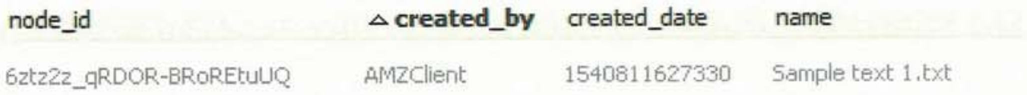


node_id	created_by	△ created_da...	name	content_.
y-_PKwbITpiLoAgSKRv5fw	CloudDriveWeb	1537735917754	Data Sample 1	xlsx

Figure 3.28 Data Sample 1.xlsx

The name is based on md5 hash value of the file. It was possible to extract the content of the file but it was not possible to determine the previous name of the file.

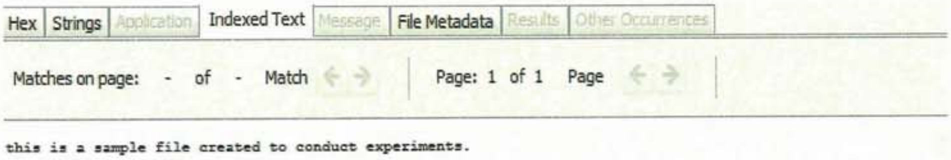
Regarding A10 (create a file), the "Sample Text 1.txt" file was found in the database file of the Amazon Drive account (amzn1.account.AF35JUUD5DEOCNYQBAMRVK6D5EDA.mixtape.db). It was created by AMZClient on October 29th, 2018 at 13:13:47 EEST (1540811627330 in Epoch time) (Figure 3.29).



node_id	△ created_by	created_date	name
6ztz2z_qRDOR-BRoREtuUQ	AMZClient	1540811627330	Sample text 1.txt

Figure 3.29 Sample Text 1.txt

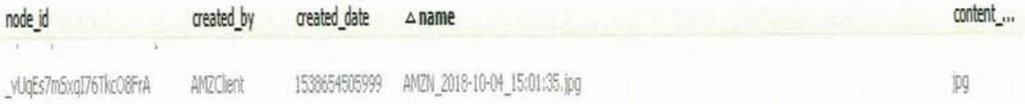
This means that the file was created by the user of the account, Laura. The text file was found in the "/data/com.amazon.drive/cache/N/NF6Vq2waTnarRt364rD1bg" directory under the name "original_1330bfcaa3f021bea1ac6ceeb93f08ed.txt". The name is made of the file's md5 hash value. The content of the file was extracted (Figure 3.30).



```
this is a sample file created to conduct experiments.
```

Figure 3.30 Content of Sample Text 1

Regarding A11 (create folder and upload photo), the "AMZN_2018-10-04_15:01:35.jpg" file was found in the database file of the Amazon Drive account (amzn1.account.AF35JUUD5DEOCNYQBAMRVK6D5EDA.mixtape.db).



node_id	created_by	created_date	△ name	content_...
_vUqEs7mSxqI76TkcO8FrA	AMZClient	1538654505999	AMZN_2018-10-04_15:01:35.jpg	jpg

Figure 3.31 AMZN_2918-10-04_15:01:35.jpg in database

It was created by AMZClient on October 4, 2018 at 15:01:45 EEST (1538654505999 in Epoch time). The node id of the file is _vUqEs7mSxqI76TkcO8FrA. The image was found in the "/data/com.amazon.drive/cache/_/_vUqEs7mSxqI76TkcO8FrA" directory under the following name "thumbnail_7edf70fb748270e0b6b4bf72e082312_2048.jpg", and its content were extracted (Figure 3.32).

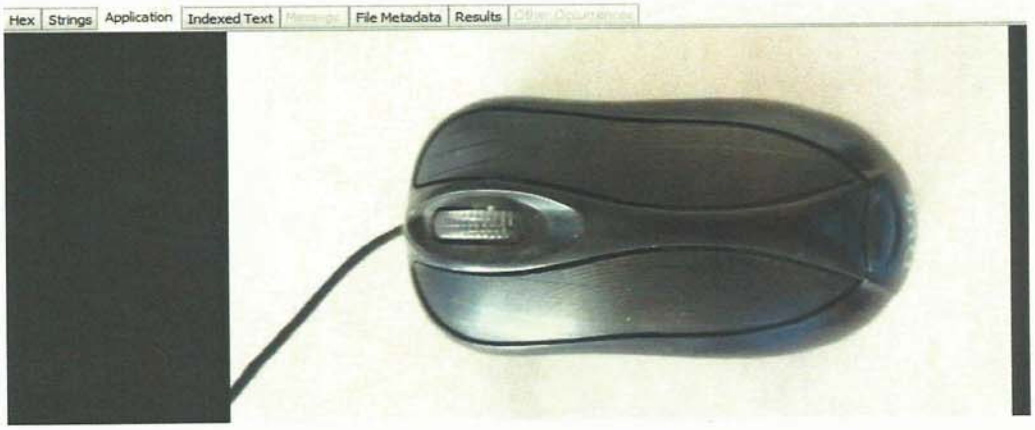


Figure 3.32 AMZN_2018-10-04_15:01:35.jpg

In addition, Personal Documents folder was found in the database file of the Amazon Drive account (amzn1.account.AF35JUUD5DEOCNYQBAMRVK6D5EDA.mixtape.db). It was created by AMZClient on October 4, 2018 at 15:00:05 EEST (1538654405641 in Epoch time). The node id of the folder is "MnP-xeT1SHKzP1sZZCWVNQ". This file's id is the parent node id of the "AMZN_2018-10-04_15:01:35.jpg" image. This indicates that the picture is uploaded to the Personal Documents folder created by the user.

3.4.4 Reporting

The reporting phase is the last phase in the digital forensic framework. In this phase, the forensic investigator provides details about the investigator, the device, the tools used in the investigation and a summary of the findings. The content of the report are kept to a minimum since the details are discussed throughout the chapter. A sample report includes the following information:

Case number: 1

Name of the investigator: Virona Nouhra.

Date of forensic examination: 1 November 2018.

Phone model: Samsung SM J500H.

Tools used for the examination: Autopsy 4.7.0

The findings of the analysis phase are shown in the graphs below and each graph is explained to show the evidence of forensic value for the investigators.

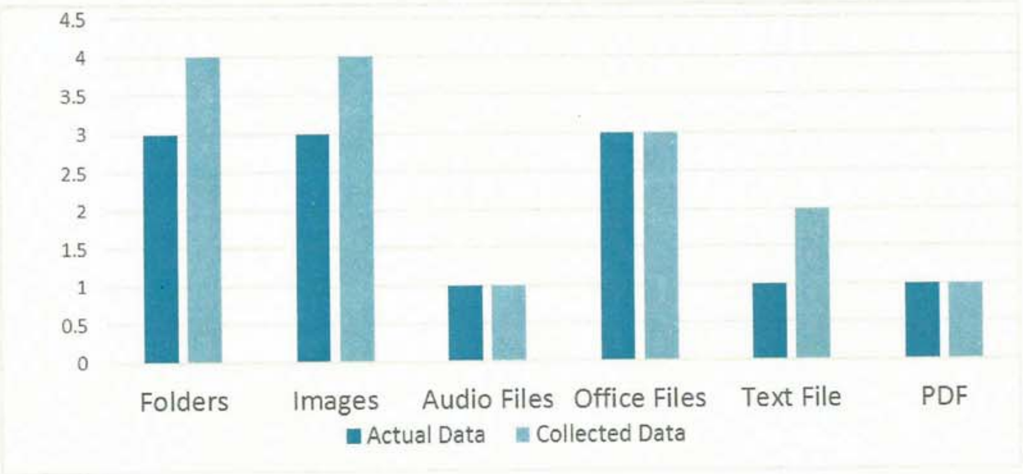


Figure 3.33 Chart showing the actual data vs the collected data

The chart presented in

Figure 3.33 shows in dark blue the actual data that can be found on the collected smartphone and in light blue the collected data after an analysis of the forensic image of the device. The chart indicates that all the audio files, PDF files and Office files are found on the device and in the collected forensic image.

However, it can be noted that the number of Folders and text files found in the forensic image was greater than the folders and text files found in the application. This is due to the fact that in the forensic image it was possible to detect deleted folders and text files.

As seen in the chart, the number of images collected from the forensic image was greater the number of images found in the application. This is because in the forensic image it was possible to find images that were inside the word document.

This graph indicates that the data collected from the forensic image is greater than that found on the application and deleted files could also be found.

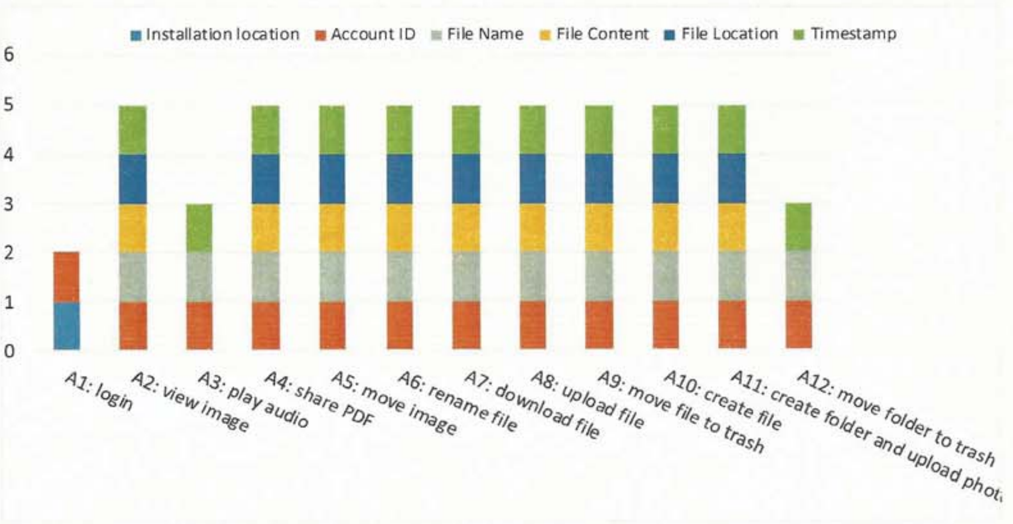


Figure 3.34 Graph representing the collected artefacts in each activity

The graph in Figure 3.34 indicates the artifacts that were found according to each activity. The legend is explained as follows: IL: installation location (where the application was installed), ACC ID: account ID (ID of the Amazon Drive account), FN: file name (name of the file), FC: file content (content of the file), FL: file location (directory where the file is stored) and timestamp (date and time).

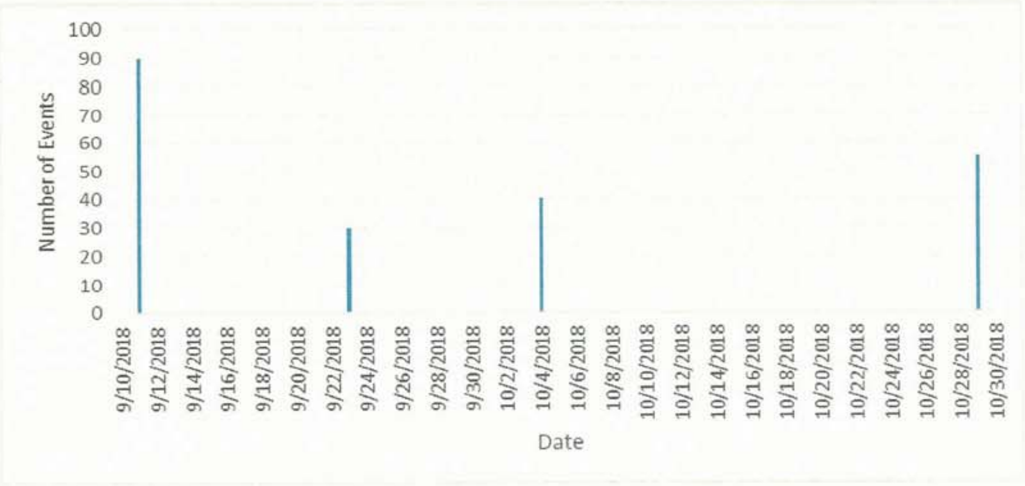


Figure 3.35 Chart showing user activity related to Amazon Account

The graph in Figure 3.35 shows the activity of the user when the experiments were conducted. It can be noted that on the 9th of September the number of events created were high since this was the date when the Amazon application was installed on the device.

On the 23rd of September, the user added files to the Amazon Drive account. This has led to an increase in the number of events connected to the Amazon application. On the 4th of October, a series of experiments were conducted by the user. This reflected an increase in the number of events on this date. At last, on the 29th of October, the user also performed some experiments leading to an increase in the number of events. It can be noted that the 29th of October is the last time the user was active on this application.

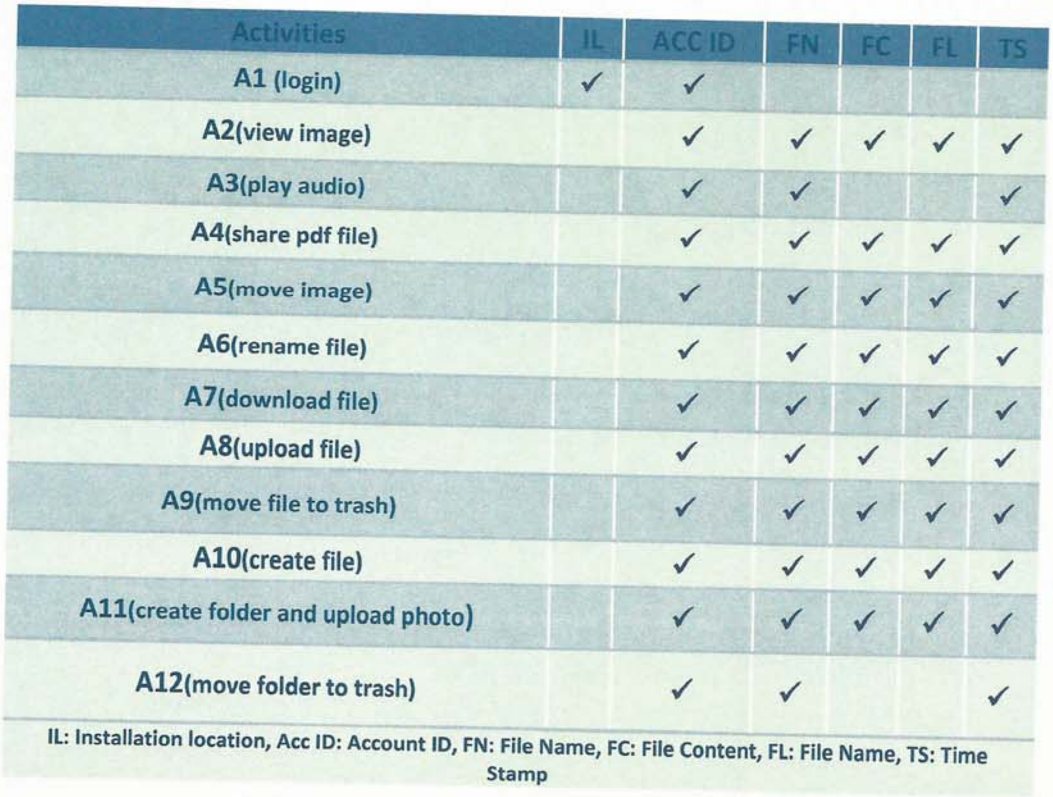
Chapter 4: Conclusion

The following chapter is a conclusion of the work. This chapter presents a table that summarizes the main results. It shows essential information about the files that were collected form the forensic image. In addition, the main contributions of the thesis are highlighted with the possible extensions and future work.

4.1 Summary of the Main Results

The findings are summarized in Table 4.1.

Table 4.1 Summary of the findings



Activities	IL	ACC ID	FN	FC	FL	TS
A1 (login)	✓	✓				
A2(view image)		✓	✓	✓	✓	✓
A3(play audio)		✓	✓			✓
A4(share pdf file)		✓	✓	✓	✓	✓
A5(move image)		✓	✓	✓	✓	✓
A6(rename file)		✓	✓	✓	✓	✓
A7(download file)		✓	✓	✓	✓	✓
A8(upload file)		✓	✓	✓	✓	✓
A9(move file to trash)		✓	✓	✓	✓	✓
A10(create file)		✓	✓	✓	✓	✓
A11(create folder and upload photo)		✓	✓	✓	✓	✓
A12(move folder to trash)		✓	✓			✓

IL: Installation location, Acc ID: Account ID, FN: File Name, FC: File Content, FL: File Name, TS: Time Stamp

This table shows the installation location for the application, account ID, file name, file location, file content and timestamp for each activity performed by the user.

When the application was installed in A1, it was possible to locate the directory where the application was installed as well as the ID of the account.

Regarding the viewing of an image without downloading it (A2), deleting a file (A4), moving an image to a folder without downloading the image (A5), renaming a file without downloading it (A6), downloading a file (A7), uploading a file to a folder without downloading it (A8), moving a file to the trash (A9), creating a file and naming it without downloading it (A10), creating a new folder and uploading a file to it without downloading the file A(11), it is possible for the forensic investigator to determine the account ID, file name, file location, file content and timestamp.

However, in activity A3, it is not possible for the forensic investigator to find the location nor the content of an audio file. But, the file name, account ID and timestamp were found in the collected forensic image.

Concerning A12 activity, when a folder is deleted, a forensic investigator cannot determine the folder location nor the folder content but the folder name, folder timestamp and account ID can be retrieved.

4.2 Main Contributions of the Thesis

The use of cloud client application like Amazon Drive can leave behind potential evidence incriminating information useful in an investigation. Without a systematic investigative procedure, crucial evidence may be missed and the integrity of the evidence compromised. In this research, we used the four-step mobile forensic guideline from NIST 10 and the four-step cloud forensic framework of Martini and Choo to guide the investigations. We demonstrated that various artefacts associated with the use of the cloud app could be recovered from the Android device's internal storage (Table 4.1).

This thesis offers a valuable contribution to forensic investigators. A large amount of artefacts was found, which could be of use in forensic investigations (including timestamp, file hash information and file content). These contributions help forensic investigators in identifying directly the location of important evidence and at the same time minimizing the time spent searching for evidence.

In addition, cloud applications usually store the user's files on servers outside the jurisdiction of the some countries. This can impede the flow of the investigation and investigators may not be given legal access to the content of the account. Therefore, this thesis helps investigators in identifying the files and folders in the account on the device itself without the need to ask for legal permission.

To the best of my knowledge, Hale conducted a forensic investigation on Amazon application on Windows XP/7, in 2013. In 2016, Easwaramoorthy et al. also conducted a research about Amazon cloud application on Windows 7 using different web browsers. In 2012, Chung et al conducted a forensic investigation about Amazon cloud application on Windows and Mac computers, as well as an iPhone and Android. This research hardly provided any information about the application on a smartphone and it did not cover any experiments nor retrieve any files. Hence, this thesis presented valuable results to forensic examiners.

4.3 Possible Extensions and Future Work

This thesis presented an investigation of the Amazon Cloud Drive application on Android operating system. File contents, file locations, file names and timestamps were reported. This thesis may serve as a stepping stone for cyber forensics investigators who will analyze the Amazon Drive application in the future.

Other studies can be conducted on smartphones running an iOS operating system. This research was only conducted on a smartphone running Android. Upon conducting an experiment with a device running an iOS operating system, artefacts can be collected to identify evidence that has forensic value.

Additional research can be done on popular cloud apps and other app categories such as: social networking, games, banking/finance, maps/navigations, and instant messaging. The aim would to contribute towards an up-to-date understanding of forensic artefacts that could be recovered from forensic investigations involving such apps.

Bibliography

Amazon. (2016a). Welcome to Amazon Drive. Retrieved December 20, 2016, from https://amazon.com/clouddrive/home

Amazon. (2016b, December 9). Amazon Drive. Retrieved December 20, 2016, from https://play.google.com/store/apps/details?id=com.amazon.drive

Amazon. (2016c, December 10). Amazon.com: Amazon Drive: Appstore for Android. Retrieved January 2, 2017, from https://www.amazon.com/Amazon-com-Amazon-Drive/dp/B00ZGCOO7W/ref=sr_1_1?ie=UTF8&qid=1483117661&sr=8-1&keywords=amazon+cloud+drive

Ayers, R., Brothers, S., & Jansen, W. (2014). Guidelines on Mobile Device Forensics. *NIST Special Publication 800-101*, (NIST publication), 85.

Barmpatsalou, K., Damopoulos, D., Kambourakis, G., & Katos, V. (2013). A Critical Review of 7 years of Mobile Device Forensics. *Digital Investigation*, *10*(4), 323–349.

Birk, D., & Wegener, C. (2012). Technical Issues of Forensic Investigations in Cloud Computing Environments. In *IEEE Sixth International Workshop on Systematic Approaches to Digital Forensic Engineering*. USA: IEEE.

Blakeley, B., Cooney, C., Dehghantanha, A., & Aspin, R. (2015). Cloud Storage Forensic: hubiC as a Case-Study. In *2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom)* (pp. 536–541). https://doi.org/10.1109/CloudCom.2015.24

Carter, B. (2014). *A Simplified Guide to Digital Evidence*. Florida, USA: National Forensic Science Technology Center.

Chelihi, A., Elutilo, A., Ahmed, I., Papadopoulos, C., & Dehghantanha, A. (2017). An Android Cloud Storage Apps Forensic Taxonomy. In *Contemporary Digital Forensic Investigations Of Cloud And Mobile Applications* (first, pp. 285–305). Elsevier.

Choo, K. K. R., & Quick, D. (2013). Dropbox analysis: Data remnants on user machines. *Digital Investigation*, *10*(1), 3–18.

Choo, K.-K. R., Martini, B., & Do, Q. (2015). Recovering Residual Forensic Data from Smartphone Interactions with Cloud Storage Providers. In *The Cloud Security Ecosystem: Technical, Legal, Business and Management issues.* (first, pp. 347–382). Boston: Elsevier.

Choo, K.-K. R., Martini, B., Herman, M., & Iogra, M. (2016). Cloud Forensics: State of the Art and Future Directions. *Digital Investigation*, *18*(Special issue), 77–78.

Choo, K.-K. R., & Quick, D. (2013). Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata? *Digital Investigation*, *10*, 266–277.

Chung, H., Park, J., Lee, S., & Kang, C. (2012). Digital Forensic Investigation of Cloud storage services. *Digital Investigation*, *9*(2), 81–95.

Damshenas, M., Dehghantanha, A., Mahmoud, R., & Bin Shamsuddin, S. (2012). Forensics Investigation Challenges in Cloud Computing Environments. In *2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensics*. Malaysia: IEEE.

Dargahi, T., Dehghantanha, A., & Conti, M. (2017). Investigating Storage as a Service Cloud Platform: pCloud as a Case Study. In *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications* (pp. 185–204). Elsevier.

Daryabar, F., Dehghantanha, A., & Choo, K.-K. R. (2017). Cloud storage forensics: MEGA as a case study. *Australian Journal of Forensic Sciences*, *49*(3), 344–357.

Dehghantanha, A., Daryabar, F., Eterovic-Soric, B., & Choo, K.-K. R. (2016). Forensic Investigation of Box, OneDrive, Dropbox and Google Drive applications on Android and iOS devices. *Australian Journal of Forensic Sciences*, *48*(6), 615–642.

Do, Q., Martini, B., & Choo, K. K. R. (2015). A Cloud-Focused Mobile Forensics Methodology. *IEEE Cloud Computing*, *2*(4), 60–65. https://doi.org/10.1109/MCC.2015.71

Duke, A. (2014, October 12). 5 Things to know about the celeb nude photo scandal - CNN.com. Retrieved January 11, 2017, from http://edition.cnn.com/2014/09/02/showbiz/hacked-nude-photos-five-things/index.html

Easwaramoorthy, S., Thamburasa, S., Samy, G., Bhushan, S. B., & Aravind, K. (2016). Digital forensic evidence collection of cloud storage data for investigation. In *2016 International Conference on Recent Trends in Information Technology (ICRTIT)* (pp. 1–6). https://doi.org/10.1109/ICRTIT.2016.7569516

EDRM. (2018). EDRM File Format Data Set. Retrieved May 31, 2018, from https://www.edrm.net/resources/data-sets/edrm-file-format-data-set/

Eoghan, C., & Brenner, S. (2011). *DIgital Evidence and Computer Crime: forensic science computer and the internet* (Third edition). London: Elsevier/ Academic press. Retrieved from http://webview.ndu.edu.lb/webview?infile=details.glu&loid=213058

Goodison, S., Davis, R., & Jackson, B. (2015). Digital Evidence and the US Criminal Justice System. RAND Corporation.

Grispos, G., Glisson, W. B., & Storer, T. (2013). Using Smartphones as a Proxy for Forensic Evidence Contained in Cloud Storage Services. In *2013 46th Hawaii International Conference on System Sciences* (pp. 4910–4919). https://doi.org/10.1109/HICSS.2013.592

Hale, J. (2013). Amazon Cloud Drive forensic analysis. *Digital Investigation*, *10*(3), 259–265.

Hidahya Ab Rahman, N., Dwi Wahyu Cahyani, N., & Choo, K.-K. R. (2017). cloud incident handling and forensic by design: cloud storage as a case study. *Concurrency and Computation: Practice and Experience*, *29*(14), 16.

Jansen, W., & Ayers, R. (2007). Guidelines on Cell Pone Forensics. *NIST Special Publication 800-101*, 104.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response. *NIST*, *10*, 800–886.

Long, C., & Qing, Z. (2015). Forensic Analysis to China's Cloud Storage Services. *International Journal of Machine Learning and Computing*, *5*(6), 467–470.

Malik, R., Shashidhar, N., & Chen, L. (2015). Cloud Storage Client Application Analysis. *International Journal of Security*, *9*(1), 1–14.

Markets&Markets. (2018). *Cloud Storage Market by Solution & Service - 2021* (p. 107). Retrieved from http://www.marketsandmarkets.com/Market-Reports/cloud-storage-market-902.html?gclid=CP_rvLKamdECFQsR0wodyScBbA

Martini, B., & Choo, K. K. R. (2013). Cloud Storage Forensics: ownCloud as a case study. *Digital Investigation*, *10*(4), 287–299.

Martini, B., & Choo, K.-K. R. (2012). An Integrated Conceptual Digital Forensic Framework for Cloud Computing. *Digital Investigation*, *9*, 71–80.

Martini, B., Choo, K.-K. R., & Do, Q. (2015). Conceptual Evidence Collection and Analysis Methodology for Android Devices. In *Cloud security ecosystem* (pp. 285–307). Elsevier.

Martini, B., Do, Q., & Choo, K.-K. R. (2015). Mobile Cloud Forensics: An Analysis of Seven Popular Android Apps. In *The Cloud Security Ecosystem: Technical, Legal, Business and Management issues.* (first, pp. 309–345). Elsevier.

Marturana, F., Me, G., & Tacconi, S. (2012). A Case Study on Digital Forensics in the Cloud (pp. 111–116). Presented at the International Conference on Cyber Ebabled Distributed Computing and Knowledge Discovery, IEEE. https://doi.org/10.1109/CyberC.2012.26

McKemmish, R. (1999). What is forensic computing. *Australian Institute of Criminology*, (Trends and issues in crime and criminal justice).

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. *800-145*, 7.

Melson, D. (2014). *Real World Mobile Forensics The Intersection of Research, Academia, and Case Work*. Presented at the Mobile forensics. Retrieved from https://www.nist.gov/sites/default/files/documents/forensics/9-Melson_Real-World-Mobile-Forensics-NIST-Presentation.pdf

Morum de L. Simao, Caus Sicoli, Peotta de Melo, & Timoteo de Sousa Junior. (2011). Acquisition of Digital Evidence in Android Smartphones. In *Australlian Digital*

Forensics Conference (Vol. 9th, pp. 116–124). Perth, Western Australia: Edith Cowan University Research Online.

Nokia. (2016). Nokia Threat Intelligence Report - 2H 2016. Retrieved March 28, 2018, from https://pages.nokia.com/8859.Threat.Intelligence.Report.html

Noyes, K. (2014). And there he stood, with a smoking datum in his hand. *Fortune*. Retrieved from http://fortune.com/2014/08/28/digital-forensics/

Oestreicher, K. (2014). A forensically robust method for acquisition of iCloud data. *Digital Investigation*, *11*, S106–S113. https://doi.org/10.1016/j.diin.2014.05.006

Quang, D., Choo, K.-K. R., & Martini, B. (2015). A Forensically Sound Adversary Model for Mobile Devices. *PLoS ONE*, *10*(9).

Quick, D., & Choo, K. K. R. (2014). Google Drive: Forensic analysis of data remnants. *Journal of Network and Computer Applicaitins*, *40*, 179–193.

Quick, D., & Choo, K.-K. R. (2013). Digital droplets: Microsoft SkyDrive forensic data remnants. *Future Generation Computer Systems*, *29*(6), 1378–1394. https://doi.org/10.1016/j.future.2013.02.001

Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M. (2011). Cloud Forensics. In *Advances in Digital Forensics 7* (1st ed., Vols. 1–361, p. 290). Orlando, Florida, USA: Springer-Verlag Berlin Heidelberg.

Samet, N., Ben letaifa, A., Hamdi, M., & Tabbane, S. (2014). Forensic Investigation in Mobile Cloud Environment. In *The 2014 International Symposium on Networks, Computers and Communications*. Tunisia: IEEE.

Scott, J. (2011, August 2). Kaspersky: Cyber criminals hide in Amazon S3 | Cloud Pro. Retrieved June 16, 2017, from http://www.cloudpro.co.uk/cloud-essentials/cloud-security/1415/kaspersky-cyber-criminals-hide-amazon-s3

Shah, J., & Malik, L. (2014). Cloud Forensics: Issues and Challenges. Presented at the 6th International Conference on Emerging Trends in Engineering and Technology, India: IEEE.

Shariati, M., Dehghantanha, A., & Choo, K. K. R. (2016). SugarSync forensic analysis. *Australian Journal of Forensic Sciences*, *48*(1), 95–117.

Shariati, M., Dehghantanha, A., Martini, B., & Choo, K.-K. R. (2015). Ubuntu One investigation Detecting evidences on client machine. In *The cloud Security Exosystem: Tehcnical, Legal, Business and Mangement Issues* (first, pp. 429–446). Elsevier.

Simou, S., Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2014). Cloud Forensics: Identifying the Major Issues and Challenge. In *CAiSE 2014: Advanced information Systems Engineering* (Vol. 8484, pp. 271–284). Springer, Cham.

Symantec. (2016). *Internet Security Threat Report* (No. 21) (p. 81). Symantec.

Teing, Y.-Y., Dehghantanha, A., Choo, K. K. R., Dargahi, T., & Conti, M. (2017). Forensic Investigation of Cooperative Storage Cloud Service: Symform as a Case Study. *Journal of Forensic Sciences*, *62*(3), 641–654.

Thamburasa, S., Easwaramoorthy, S., Aravind, K., Bhushan, S. B., & Moorthy, U. (2016). Digital forensic analysis of cloud storage data in IDrive and Mega cloud drive. In *2016 International Conference on Inventive Computation Technologies (ICICT)* (Vol. 3, pp. 1–6). https://doi.org/10.1109/INVENTIVE.2016.7830159